

Version 5.2.4

SurfControl RiskFilter - E-mail Administrator's Guide



CONTENTS

Notices	i
FINDING YOUR WAY AROUND	1
Managing your messages with RiskFilter	∠
	4
Launching SurfControl RiskFilter	6
RiskFilter System Management Console	6 7
RiskFiller Management Console (Administrator)	/
Belore you start	8
System Settings	9
The System Settings tab	10
Terminology used	10
What can be configured in the System Settings tab?	10
General	11
Configuration	11
User Directories	13
Secure Proxy	22
Logs and Archives	24
	25
Receive Settings	27
Connection Control	27
Directory Attack Control	29
Relay Control	3U 22
Message Control	33 34
Exception Control	
Black List	
White List	
Send Settings	41
Domain-Based Delivery	41
Traffic Control	43
Advanced Delivery	43
User Management	45
Account Manager	45
Personal E-mail Manager	48
End-user Control	52
User Authentication	53
License & Updates	55
Update Now	55
Scheduled Update	57
License Status	58
Update Server	59
	60

i

Help	61
Admin Guide	61
Contact Support	61
Firstboot Wizard	62
Configuration Wizard	62
Key Points	63
	65
The Policy Manager tab	
l erminology used	
what can be configured in the Policy Manager tab?	
Creating a Policy	67
Step 1 - Defining users	67
Step 2 - Defining the action	
Step 3 - Defining the Rules	68
Address Group	69
Importing and exporting Lists	69
Deleting Address groups	70
Queue Manager	71
Adding Queues	71
Dictionary Manager	
SurfControl Dictionaries	
Custom Dictionaries	
Importing dictionaries	
Global Policy	79
Creating a new Sub-policy	79
Editing a sub-policy	81
Adding Filters to the policy	81
Defining a filter	
The Anti-Virus Agent Filter	
The Anti-Spam Agent Filters	
Internet Threat Database Filter	
Standard Disclaimer	
General Content Filter	
advanced content filter	
Message Attachment Filter	
Content Guardian	
Dictionary Threshold Filter	
Key Points	103
REPORTS & LOGS	105
The Reports and Logs tab	
rerminology used	
what can be configured in the Reports and Logs tab?	
Dasnboard	
Master Report	
Querying the Master Report	
Message Report	

Querying the Message Report	110
Policy Report	111
Querying the Policy Report	.111
Virus Report	112
Querving the Virus Report	.112
Snam Report	113
Ouerving the Spam Report	113
Connection Deport	11/
Ouerving the Connection Report	114
	440
System Report	116
Isolated Messages	117
Managing Isolated Messages	117
Virus Messages	119
Managing the Virus Messages	119
Spam Messages	121
Managing Spam Messages	121
Archived Messages	123
Managing Archived Messages	123
Deferred Messages	127
Querving Deferred Messages	127
Key Points	120
	120
	1 2 1
	121
Overview	132
Overview	132
Overview What can be configured with the System Management Console? Accessing the RiskFilter System Management Console	132 132 133
Overview What can be configured with the System Management Console? Accessing the RiskFilter System Management Console The rfmngr account	132 132 133 133
Overview. What can be configured with the System Management Console? Accessing the RiskFilter System Management Console The rfmngr account The Webmin Tab	132 132 133 133 134
Overview What can be configured with the System Management Console? Accessing the RiskFilter System Management Console The rfmngr account The Webmin Tab What can be configured in the Webmin tab?	132 132 133 133 134 134
Overview What can be configured with the System Management Console? Accessing the RiskFilter System Management Console The rfmngr account The Webmin Tab What can be configured in the Webmin tab? Webmin Actions Log	132 132 133 133 134 134 135
Overview What can be configured with the System Management Console? Accessing the RiskFilter System Management Console The rfmngr account The Webmin Tab What can be configured in the Webmin tab? Webmin Actions Log Webmin Configuration	132 132 133 133 134 134 134 135 135
Overview What can be configured with the System Management Console? Accessing the RiskFilter System Management Console The rfmngr account The Webmin Tab What can be configured in the Webmin tab? Webmin Actions Log Webmin Configuration Webmin Servers Index	132 133 133 134 134 135 135 135
Overview What can be configured with the System Management Console? Accessing the RiskFilter System Management Console The rfmngr account The Webmin Tab What can be configured in the Webmin tab? Webmin Actions Log Webmin Configuration Webmin Servers Index	132 133 133 134 134 135 135 135 137 138
Overview	132 133 133 134 134 135 135 135 137 138 138
Overview	132 133 133 134 134 135 135 135 137 138 138 139
Overview	132 133 133 134 134 135 135 135 135 137 138 138 139 139
Overview	132 133 133 134 134 135 135 137 138 138 139 139 139
Overview	132 133 133 134 134 135 135 135 135 137 138 139 139 139 140
Overview What can be configured with the System Management Console? Accessing the RiskFilter System Management Console The rfmngr account The rfmngr account What can be configured in the Webmin tab? Webmin Actions Log Webmin Configuration Webmin Servers Index The System Tab What can be configured in the System tab? Bootup and Shutdown Change Passwords Historic System Statistics Multi Gateway Policy Routing Network Configuration	132 133 133 134 134 135 135 135 135 137 138 139 139 139 140 141
Overview	132 133 133 134 134 135 135 135 135 137 138 139 139 139 139 140 141 146
Overview	132 133 133 134 134 135 135 135 137 138 139 139 139 139 140 141 146 146
Overview	132 133 133 134 134 135 135 137 138 139 139 139 139 139 140 141 146 146 147
Overview	132 133 133 134 134 135 135 135 135 137 138 139 139 139 140 141 146 146 147 148
Overview	132 133 133 134 134 135 135 135 135 135 135 137 138 139 139 140 141 146 146 147 148 148
Overview	132 133 133 134 134 135 135 135 135 135 137 138 139 139 139 140 141 146 146 147 148 148 149
Overview	132 133 133 134 134 135 135 135 135 137 138 139 139 139 139 139 140 141 146 146 147 148 149 149
Overview	$\begin{array}{c} 132 \\ 132 \\ 133 \\ 133 \\ 134 \\ 135 \\ 135 \\ 137 \\ 138 \\ 139 \\ 139 \\ 139 \\ 139 \\ 140 \\ 141 \\ 146 \\ 147 \\ 148 \\ 149 \\ 149 \\ 149 \\ 150 \end{array}$

Update RiskFilter - E-mail	154
Key Points	155
APPENDIX	157
Using the Command Line Interface	
gtool.sh	
uninstall.sh	
Internet Threat Database Categories	
Core / Liability Categories	
Productivity Categories	
INDEX	

Finding your way around

How RiskFilter works	page 2
Load balancing with RiskFilter	page 4
Launching SurfControl RiskFilter	page 6
Before you start	page 8



How RISKFILTER WORKS

Figure 1-1shows how a message is processed by RiskFilter:



Figure 1-1 The RiskFilter filtering process

MANAGING YOUR MESSAGES WITH RISKFILTER

RiskFilter gives you access to several tools with which you can manage your E-mail messages:

Component	What it does	Find out more
Queues	Any isolated e-mails are moved to different queues (depending on the the type of message) for safe keeping. You can then release, move or delete them. These directories also show the activity logs.	See Queue Manager in the Policy Manager chapter.
Filters	Filters govern whether a message should be delivered or isolated. Use the supplied filters: Anti-Virus, Anti-Spam and Internet Threat Database, or create your own custom filters to catch specific messages.	See Global Policy > Adding Filters to the Policy in the Policy Manager chapter.

Table 1-1 RiskFilter Core Components



Table 1-1 RiskFilter Core Components

Component	What it does	Find out more
Connection Control	Limit the number of simultaneous connections made on your server. Determine whether to perform real-time blacklist checking.	See Receive Settings > Connection Control in the System Settings chapter.
Dictionary Management	Dictionaries are used by the filters to detect particular kinds of content – use Dictionary Management to configure Dictionaries to suit your needs.	See Dictionary Manager in the Policy Manager chapter.
Relay Control	Stop your e-mail system from being used as an open relay by spammers.	See Receive Settings > Relay Control in the System Settings chapter.



LOAD BALANCING WITH RISKFILTER

You can deploy RiskFilter in a cluster and load-balance using MX records:

- 1 On the DNS server hosting your domain, create an MX record for each primary RiskFilter server using the same MX preference.
- 2 Give the failover server a higher number. This will give it a lower preference.

Table 1-1 shows an example of MX preference assignments for load-balancing and failover using MX records.

Table 1-1	Usina MX	Records for	Load-Balancing
	Conig mix	1 100001 000 101	Loud Dulationing

Mail Exchanger	IP Address	MX Preference
Site A		
mx1.siteA.com	208.126.216.20	5
mx2.siteA.com	208.126.216.21	5
mx3.siteA.com	208.126.216.22	5
mx4.siteA.com	197.201.56.201	10
Site B		
mx1.siteB.com	197.201.56.201	5
mx2.siteB.com	197.201.56.202	5
mx3.siteB.com	197.201.56.203	5
mx4.siteB.com	208.126.216.20	10



Figure 1-2 Load balancing



A lower MX preference number gives higher priority than a lower one. In Figure 1-2, e-mail is sent in the following way:

- E-mail sent to site A.com round-robins between mail exchangers 1, 2, and 3, because each RiskFilter appliance has the same MX preference of 5.
- The same thing happens for e-mail sent to site B.com. If site A is down (e.g., with a network failure), the sending mail server will route e-mail to the fourth (failover) MX record, which is the address of a server in a different physical location.

For the described failover to work properly, RiskFilter appliances at site A are configured to accept messages for site B, and RiskFilter appliances at site B are configured to accept messages for site A.

The failover servers have static routes configured so that RiskFilter knows where to route the e-mail. There are also advanced load-balancing switches that can be used for these purposes. These switches offer a variety of load-balancing algorithms, in addition to round-robin delivery, which provide efficient load distribution and timely failover. Using load-balancing switches may improve the overall efficiency of your SMTP infrastructure.



LAUNCHING SURFCONTROL RISKFILTER

SurfControl RiskFilter consists of two interfaces:

- RiskFilter System Management Console
- RiskFilter Management Console (Administrator)

There is also a third interface available to users if you enable Personal E-mail Manager (PEM). This enables them to manage spam messages that have been isolated (See "Personal E-mail Manager" on page 48 for more details).



Note: All text fields within RiskFilter can accept non-Latin characters such as Japanese. However, there is a text-limit of 64 characters within these fields. Any values entered into these fields such as port and refresh rates, must be valid integers.

RISKFILTER SYSTEM MANAGEMENT CONSOLE

The RiskFilter System Management Console enables you to configure the RiskFilter appliance itself as well as its interaction with the surrounding network. With RiskFilter System Management Console you can:

- Use IP Access Control to only allow access to those IP addresses that you trust.
- Make changes to the language that titles, prompts and messages etc will be displayed in, within the RiskFilter appliance interfaces.
- Make network specific changes, such as adding RiskFilter Management Console servers and specifying which IP addresses and ports RiskFilter Management Console will bind to.
- Keep records of the various actions taken by administrators on the RiskFilter Management Console server.
- · Check things like historic system settings and running processes.
- Change passwords.

To open the RiskFilter System Management Console:

3 Open a web browser and type:

https://<hostname_or_ipaddress>:10000/

where '<hostname_or_ipaddress> is the name or IP address of your RiskFilter appliance.

- 4 At the RiskFilter Management Console login page enter the username and password. The default username and password are:
 - Username = rfmngr
 - Password = \$rfmngr\$
- 5 Click Login.

See "RiskFilter System Management Console" on page 131 for detailed information on all of RiskFilter Management Console's functionality and how to use the interface.

RISKFILTER MANAGEMENT CONSOLE (ADMINISTRATOR)

The SurfControl RiskFilter Management Console is where you manage the RiskFilter software. You can use this interface to:

- Manage user accounts and licensing.
- Schedule updates to Anti-Virus and Anti-Spam agents.
- Manage servers and connection issues.
- · Set up policies to manage how users send and receive e-mail.
- Run reports on these users and their messages.

To open the RiskFilter Management Console:

1 Open a web browser and type:

https://<hostname_or_ipaddress>/admin where '<hostname_or_ipaddress> is the name or IP address of your RiskFilter appliance.

- 2 At the RiskFilter Management Console login page enter the user name and password that you want to use to access the account. The default user name and password are:
 - User name = administrator
 - Password = admin
- 3 Click Login.

Opening the RiskFilter Management Console

As soon as the RiskFilter Management Console opens, you will see the Dashboard containing brief information about servers used, as well as a report showing general e-mail use:

Dashboard	
	Refresh
Server	Status
lasa.surfcontrol.com	Normal
Mail Server	Status
192.168.86.22:255	Online
LDAP Server	Status
192.168.86.22	Online
192.168.86.17	Online
	Past 7 days 💌
Master Report	
800	





BEFORE YOU START

This Administrator's guide assumes that you have completed the following steps:

- 1 Mounted the appliance using the supplied hardware set up guide.
- 2 Gathered the network information that is required for the configuration of the RiskFilter appliance.
- 3 Configured the RiskFilter appliance via your chosen connection, using the network information that you gathered earlier. The RiskFilter Starter guide contains details of the different connection options.
- 4 Updated the SurfControl OS and software using the RiskFilter Management Console.
- 5 Activated your RiskFilter license.
- 6 Updated the Anti-Virus and Anti-Spam agents.
- 7 Configured Relay Control and e-mail-routing.

For instructions on how to carry out these steps refer to the Starter Guide which is supplied with the RiskFilter appliance.

System Settings

The System Settings tab	page 10
General	page 11
Receive Settings	page 27
Send Settings	page 41
User Management	page 45
Help	page 61
Key Points	page 63



The System Settings tab

This chapter explains how to use the System Settings tab to:

- Configure the transport of e-mails.
- Authenticate the senders and recipients of e-mails.

TERMINOLOGY USED

The following terminology is used in this chapter:

- **PEM** Personal E-mail Manager. Enables users to manage their own isolated messages.
- User Directories Provides RiskFilter with recipient address validation and end-user authentication.
- ESMTP Extended Simple Mail Transfer Protocol. Enhances SMTP by specifying extensions for sending e-mail to support graphics, audio and video files. It also enables SMTP to support the sending of text in various national languages.
- CSR Certificate Signing Request. Contains the public key information which matches the private key
 installed on RiskFilter and enables you to import a new certificate. When the CSR is exported to the
 same directory as the new certificate, the certificate will pick up this information so that RiskFilter can
 recognize it.
- **AVA** Anti-Virus Agent
- ASA Anti-Spam Agent

WHAT CAN BE CONFIGURED IN THE SYSTEM SETTINGS TAB?

The System Settings tab is where you configure the receiving and delivery of messages to and from the RiskFilter appliance.



Figure 2 - 1 The System Settings Tab

System Settings enables you to:

- · Configure user authentication and directories for storing messages and log files
- Set up Personal E-mail Manager (PEM)
- Set up a postmaster e-mail address
- · Configure sending and receiving information
- · Set up licensing and updates



GENERAL

The General menu contains sub-menus that enable you to set up the delivering and receiving of e-mails. This includes specifying how RiskFilter should treat connections from other administrators, and where to send alert messages and notifications.

CONFIGURATION

These settings are added in the **Configuration** screen.

Configuration	
SMTP Greeting Message	
SMTP Greeting Message	Welcome to lasa have a good time
STARTTLS Advertisement	Check this option to enable STARTTLS advertisement in the EHLO command response
Notification Email Addresses	
Administrator E-mail	stafford.home@surfcontrol.com
	e.g., postmaster@yourcompany.com (this e-mail address will receive system warning messages)
Default Notification Sender E-mail	stafford.horne@shorne.surfcontrol.com
	e.g., admin@yourcompany.com (this e-mail address will be used for sending notification messages)
Admin Console	
Preferred MIME Charset	Unicode(UTF-8)
Admin Console Locale	English
Admin Console Session Timeout	600 minutes (Range: 5-600) *
Trusted IP(s)	
	Allow access to the admin console only from the above IP address(es). Empty means accessible from any IP address. Separate multiple IP addresses with a semicolon(;).
	Submit Reset

Figure 2 - 2 The Configuration screen

Postmaster e-mail address

If a service stops, or a similar event occurs, RiskFilter can send a warning message to a predefined address. This predefined postmaster e-mail address is usually the administrator's.

To set up the Postmaster e-mail address:

- 1 Select General > Configuration from the System Settings tab.
- 2 Enter the e-mail address of the administrator into the **Administrator E-mail** field. This is the address that will receive the system warning messages.
- 3 Enter the e-mail address of the administrator into the **Default Notification Sender E-mail** field. Notifications will be sent to the user from this address, informing them that the message has been isolated.
- 4 Click **Submit**. For information on the other settings that can be entered into this screen see Table 1 on page 12.



Table 1 Other Settings

Setting	What it does
SMTP greeting message	The greeting message can indicate that the system is working correctly when you first start to set up the RiskFilter appliance using Hyper Terminal. An example of where this message appears would be: [root@smg10 conf]# telnet localhost 25 Trying 127.0.0.1 Connected to localhost. Escape character is '^]'. 220 Surfcontrol RiskFilter ESMTP Service Ready To set a new message, enter this message into the SMTP greeting message field.
Admin Console Locale	 Set the language that is used within RiskFilter by choosing one of the options: User Language specified by Browser - RiskFilter will select the language automatically according to the browser's language setting. English Simplified Chinese Japanese
Preferred MIME Charset	Select the MIME Charset which will be used to encode mail. We recommend that you select ISO 8859-1.
Admin Console Session Timeout	If the administrator connects to the RiskFilter appliance then leaves the connection idle, the connection will be dropped after a certain amount of time. To set this timeout, enter the length of time in minutes into the RiskFilter Console Session Timeout field.



USER DIRECTORIES

User Directories provide RiskFilter with recipient address validation and end-user authentication:

- Address validation takes place when a message is received.
- User authentication is used by end-users to log in and check their isolated messages.

To add User Directories:

- 1 Select General > User Directories from the System Settings tab.
- 2 Click Add.
- 3 Select your Directory Type from the list of options.

Create a User Directory	
- This screen enables the administrator to create new User Directory. Please select a directory type and press Ni	ext.
Select a Directory Type	
Microsoft Active Directory ■	
O IBM LDAP Server	
O Generic LDAP	
OESMTP	
O Recipient File	
O Local Database	
	Next Cancel

Figure 2 - 3 Defing the type of directory you want to create

- 4 Enter details into the screen that follows according to the type of User Directory you are adding.
- 5 Click Submit.

Editing User Directories

Once you have added your User Directory you can edit it at any time providing you have not configured Recipient Validation or User Authentication. If you have added either of these, the directory ID of the User Directory cannot be edited.

To edit a User Directory:

1 In the User Directories screen click the Edit button alongside the directory you want to edit:

User Directories			
User Directories provide Ri validation takes place as th isolated spam messages.	skFilter - E-mail with recipient e-mai e message is received while user a	l address validation and user e-mail account a uthentication is used to enable end-users to lo	authentication. Recipient og in and check their
Directory ID	Server Type	Details	
LASA Sendmail	ESMTP	- Edit	
Yamin Com	Generic LDAP	Edit	
Local PERL	ESMTP	Edit.	
us DB	Local Database	Edit	
sendmail	ESMTP	- Edit	
LDB	Local Database	Edit	
New DB	Local Database	Edit	
DB2	Local Database	Edit	
IBM-ESMTP	ESMTP	Edit	
corina	Local Database	Edit	
			Add Delete

Figure 2 - 4 Existing User Directories



2 This will show a screen containing all of the details of the User Directory that you want to edit. The following example shows a Generic LDAP User Directory:

Conceile L DAD Conversion		
Generic LDAP Serv	er Information	
This screen enables you to This directory supports Add	o configure a Generic LDAP user directory (see the RiskFilter - E-mail Administrator's Guide for more details). dress Group Import, User Authentication, User Aliases and Recipient Validation.	
Directory Information		
Directory ID	Yamin Com • (in use)	
Server Address	127.0.0.1	
Port	389 •	
	Enable Secure LDAP	
User Name	cn=manager,dc=yamin,dc=c *	
Password	•••••	
LDAP Search Setting	S	
Base DN	dc=yamin,dc=com *	
Search Filter	(mail=%email%) *	
Mail Field	mail;proxyAddresses *	
General Settings		
Cache Setting	 ○ Cache All Addresses ⊙ Enable Partial Address Caching Maximum Cache Entry 10000 * ○ Disable Address Caching 	
Cache Timeout	60 * minute(s)	
	Submit Reset	

Figure 2 - 5 Generic LDAP Server Information

- 3 Make changes to the User Directory by editing these details.
- 4 Click **Submit** to save the changes or click **Reset** to undo any changes that you have made.

Deleting a User Directory

You can delete any User Directory you have added providing you have not configured Recipient Validation or User Authentication. If you have added either of these, the User Directory cannot be deleted.

To delete a User Directory:

1 Open the User Directories screen.

	User Directories			
:	User Directories provide RiskFilter - E-mail with recipient e-mail address validation and user e-mail account authentication. Recipient validation takes place as the message is received while user authentication is used to enable end-users to log in and check their isolated spam messages.			
	Directory ID	Server Tyne	Details	
l	LASA Sendmail	ESMTP	- Edit	
	Yamin Com	Generic LDAP	Edit.	
L	Local PERL	ESMTP	Edit	

Figure 2 - 6 Existing User Directories

- 2 Select the check box alongside the User Directory that you want to delete.
- 3 Click Delete.

The following sections cover the different types of user directories that you can add to RiskFilter and the information you need to add.



Microsoft Active Directory

This is the default server type. Microsoft Active Directory supports Address Group Import, User Authentication, User Aliases and Recipient Validation.

To add a Microsoft Active Directory server:

- 1 Click Add in the User Directories screen.
- 2 Make sure that the default **Microsoft Active Directory** option is selected.
- 3 Click Next. The Microsoft Active Directory Server Information screen is displayed.

Microsoft Active Directory Server Information		
This screen enables you to cases, but can be modified Address Group Import, Us	o configure a Microsoft Active Directory user directory. The default search filter below should work in most d if necessary (see the RiskFilter - E-mail Administrator's guide for more details). This directory supports er Authentication, User Aliases and Recipient Validation.	
Directory Information		
Directory ID		
Server Address	*	
Port	389 •	
	Enable Secure LDAP	
User Name	•	
Password		
LDAP Search Setting	5	
Base DN	x	
Search Filter	(](mail=%email%)(userPrincipalName=%email%)(proxyAddresses=smtp:%email%))	
General Settings		
Cache Setting	 ○ Cache All Addresses ⊙ Enable Partial Address Caching Maximum Cache Entry 10000 ▲ ○ Disable Address Caching 	
Cache Timeout	60 * minute(s)	
	Submit Reset	

Figure 2 - 7 Microsoft Active Directory Server Information

- 4 Enter the following information:
 - Directory ID The ID of the directory. This field is limited to 64 characters.
 - Server Address The address of your LDAP server.
 - **Port** The default is 389.
 - Enable Secure LDAP Select the check box if you wish to enable Secure LDAP. This will change the default port number to 636.
 - User Name / Password The user name and password for this appliance.
 - **Base DN** This is the Base DN of the LDAP server when applying the validation filter. It can contain any of the above variables.
 - Search Filter The search filter is a standard LDAP query and can also use the variables listed. For example: |(mail=%email%) (user=%user%) (ou=Engineering)
 - Cache Setting Select the option that corresponds to how you want to treat Address Caching:
 - Cache All Addresses All addresses will be cached.



- Enable Partial Address Caching This is the default setting. Enter a value into the Maximum Cache Entry field to specify how many entries should be stored in the memory cache. The default is 10000.
- Disable Address Caching No addresses will be cached.
- Cache timeout When Cache All Addresses or Enable Partial Address Caching are enabled, addresses of all e-mails passing through RiskFilter are checked against the validation server.
 E-mails from valid addresses are delivered, and the addresses held in cache for a set time. If an e-mail is sent from a previously validated address within this cache timeout, the e-mail is delivered without contacting the validation server. However, if another e-mail is sent from this address after the cache timeout, the server will be contacted again to validate the address. This setting must be in valid Integers. The default is 60.

IBM LDAP server

IBM LDAP supports Address Group Import, User Authentication, User Aliases and Recipient Validation. If you use a server running IBM LDAP authentication, you can add an IBM LDAP server.

To add an IBM LDAP server:

- 1 Click **Add** in the User Directories screen.
- 2 Select **IBM LDAP Server**.
- 3 Click **Next**. The IBM LDAP server screen is displayed.
- 4 Enter the following information:
 - Directory ID The ID of the directory. This field is limited to 64 characters.
 - Server Address The address of your LDAP server.
 - Port The default is 389.
 - Enable Secure LDAP Select the check box if you wish to enable Secure LDAP. This will change the default port number to 636.
 - User Name / Password The user name and password for this appliance.
 - Cache Setting Select the option that corresponds to how you want to treat Address Caching:
 - Cache all addresses All addresses will be cached.
 - Enable Partial Address Caching This is the default setting. Enter a value into the Maximum Cache Entry field to specify how many entries should be stored in the memory cache. The default is 10000.
 - Disable Address Caching No addresses will be cached.
 - Cache timeout When Cache All Addresses or Enable Partial Address Caching are enabled, addresses of all e-mails passing through RiskFilter are checked against the validation server.
 E-mails from valid addresses are delivered, and the addresses held in cache for a set time. If an email is sent from a previously validated address within this cache timeout, the e-mail is delivered without contacting the validation server. However, if another e-mail is sent from this address after the cache timeout, the server will be contacted again to validate the address. The default is 60.
- 5 Click **Submit**.

Generic LDAP

Generic LDAP supports Address Group Import, User Authentication, User Aliases and Recipient Validation.

To add an Generic LDAP server:

- 1 Click Add in the User Directories screen.
- 2 Select Generic LDAP.
- 3 Click Next. The Generic LDAP screen is displayed.
- 4 Enter the following information:
 - Directory ID The ID of the directory. This field is limited to 64 characters.
 - Server Address The address of your LDAP server.
 - **Port** The default is 389.
 - Enable Secure LDAP Select the check box if you wish to enable Secure LDAP. This will change the default port number to 636.
 - User Name/ Password The user name and password for this appliance.
 - **Base DN** This is the Base DN of the LDAP server when applying the validation filter.
 - Search Filter The search filter is a standard LDAP query and can also use the variables listed. For example: |(mail=%email%) (user=%user%) (ou=Engineering)
 - Mail Field The field in the LDAP query that contains the e-mail address to be imported.
 - Cache Setting Select the option that corresponds to how you want to treat Address Caching:
 - Cache All Addresses All addresses will be cached.
 - Enable Partial Address Caching This is the default setting. Enter a value into the Maximum Cache Entry field to specify how many entries should be stored in the memory cache. The default is 10000.
 - **Disable Address Caching** No addresses will be cached.
 - Cache Timeout When Cache All Addresses or Enable Partial Address Caching are enabled, addresses of all e-mails passing through RiskFilter are checked against the validation server. Emails from valid addresses are delivered, and the addresses held in cache for a set time. If an email is sent from a previously validated address within this cache timeout, the e-mail is delivered without contacting the validation server. However, if another e-mail is sent from this address after the cache timeout, the server will be contacted again to validate the address. The default is 60.
- 5 Click Submit.



Validation settings

Variables which can be used for validation. These can be set when you are adding your LDAP server.

Search Filter. There are three variables which can be used in the Search filter for validation:

- %user% = the user name of the user to be validated
- %domain% = the domain that this user belongs to
- %email% = the e-mail address of this user

LDAP will try to validate a message by checking with the LDAP server using this search, for example: jbloggs@mycom.com

This message will be validated using the variables as follows:

- %user%=jbloggs
- %domain%= mycom.com
- %email%=jbloggs@mycom.com

Base DN. BaseDN, is an LDAP term meaning the base Domain Name which will be in the form of:

cn=users,dc=example,dc=com

Mail Field. The mail field is a list of LDAP entries containing e-mail addresses. When importing address groups, the mail field is used to find out which entries/field in the LDAP server are e-mail addresses.

ESMTP Server Information

ESMTP adds many enhancements to the SMTP protocol such as security and authentication. It supports User Authentication and Recipient Validation.

To add an ESMTP server:

- 1 Click Add in the User Directories screen.
- 2 Select ESMTP.
- 3 Click **Next**. The ESMTP Server Information screen is displayed.
- 4 Enter the following information:
 - Directory ID The ID of the directory. This field is limited to 64 characters.
 - Server Address The address of your ESMTP server.
 - Enable secure connection using STARTTLS Allow validation and authentication using TLS



Note: SurfControl recommends that STARTTLS is enabled for security reasons. Using TLS may, however, have some impact on performance, as extra CPU processing is needed to encode and decode the TLS encrypted data.

- Port The default port is 25.
- E-mail Verification Method Select the option that corresponds to how you want e-mail to be verified:
 - Use the return status of the VRFY command
 - Use the return status of the RCPT command



- Cache Setting Select the option that corresponds to how you want to treat Address Caching:
 - Enable Partial Address Caching This is the default setting. Enter a value into the Maximum Cache Entry field to specify how many entries should be stored in the memory cache. The default is 10000.
 - Disable Address Caching No addresses will be cached.
- Cache Timeout When Enable Partial Address Caching is enabled, addresses of all e-mails
 passing through RiskFilter are checked against the validation server. E-mails from valid addresses
 are delivered, and the addresses held in cache for a set time. If an e-mail is sent from a previously
 validated address within this cache timeout, the e-mail is delivered without contacting the
 validation server. However, if another e-mail is sent from this address after the cache timeout, the
 server will be contacted again to validate the address. The default is 60.
- 5 Click Submit.

Recipient File

You can validate a user ID with a recipient address file. Recipient file supports Address Group Import, as well as Recipient Validation. In addition, you can save user addresses as a text file (one e-mail address per line), for user recipient validation.

To add Recipient File validation:



- 1 Click Add in the User Directories screen.
- 2 Select Recipient File.
- 3 Click Next. The Recipient File screen is displayed.
- 4 Enter a name for the Recipient File into the Directory ID field. This field is limited to 64 characters.
- 5 Click **Browse** to navigate to your list of e-mail addresses.



Note: These must be text format, with one address per line.

- 6 Locate the file then click **Open**.
- 7 Click Submit.

Local Database

A user-defined list of e-mail addresses and passwords can be imported onto the RiskFilter appliance and stored in the database for authentication and validation purposes. Local Database supports Address Group import, Recipient Validation and User Authentication if a password is set.



Note: The text file that you want to import names and e-mail addresses from should be a plain text file (.txt) or an Excel file in csv format. Users' e-mail addresses and passwords must be separated by a semi-colon (;), space, tab or comma (,).



To add a local database:

- 1 Click Add in the User Directories screen.
- 2 Select Local Database.
- 3 Click **Next**. The Local Database Information screen is displayed:

Local Database Information	
This screen enables you to configure a local DB user directory which can be used if you do not have an LDAP server (see the RiskFilter - E-mail Administrator's Guide for more details). This user directory supports Address Group import, Recipient Validation and User Authentication if a password is provided.	
Directory Information	
Directory ID	•
File path	File format: one item per line, one item will contain one email address and password combination, if required, delimited by space, or tab, or "," or ","
	Contains Password
General Settings	
Cache Setting	O Cache All Addresses ○ Disable Address Caching
	Submit

Figure 2 - 8 Local Database Information

- 4 Enter the following information:
 - Directory ID The ID of the directory. This field is limited to 64 characters.
 - File Path The path to the database. Enter the path or click Browse to navigate to it.



Note: You can create a user directory for Local Database without the database path being specified, then create and add the actual database manually, later. Just leave the File Path field blank when you are creating the user directory.

- 5 Select the 'Contains Password' check box if the file being imported contains passwords which you want to use:
 - If you create a local database with a password, then this local database can be used for Recipients Validation and User Authentication.
 - If you create a local database with no password, then this local database can be used for Recipients Validation.



Note: Once you have selected or cleared the 'Contains Password' check box, it cannot be subsequently altered. You must create a new Local Database User Directory in order to change it.

- 6 Set up address validation caching for the RiskFilter appliance in the General Settings section by choosing one of the following options:
 - Cache All Addresses All addresses will be cached.
 - **Disable Address Caching** Addresses will not be cached.
- 7 Click **Submit**.



Adding addresses to a local database. You can add specific addresses from a user list by adding them manually. This can also be used if you have created your user directory before you created your user list and now want to add this list to the user directory.

To add addresses manually:

- 1 Create your database and store it in a place accessible to RiskFilter.
- 2 In the User Directories screen select the User Directory you want to add the addresses to.

LDB Local Database 💽 🔽

3 Click Edit. The Local Database Information screen is displayed.

Local Database Information		
This screen enables yo Administrator's Guide fr password is provided.	u to configure a local DB user directory which can be used if you do not have an LDAP server (see the RiskFilter - E-mail or more details). This user directory supports Address Group import, Recipient Validation and User Authentication if a	
Directory Informati	on	
Directory ID	LDB *	
File path	Browse File format: one item per line, one item will contain one email address and password combination, if required, delimited by space, or tab, or "," or ","	
	Contains Password	
Total Addresses	2	
General Settings		
Cache Setting	 O Cache All Addresses ○ Disable Address Caching 	
	Submit Addresses Rese	

Figure 2 - 9 Local Database Information

- 4 Click **Browse** and browse to the database containing the addresses that you want to add. Alternatively, enter the path to the file in the File path field.
- 5 Click Addresses. The Local Database Addresses screen is displayed.

Local Database - Addresses			
This screen enables you to configure a local DB user directory which can be used if you do not have an LDAP server (see the RiskFilter - E-mail Administrator's Guide for more details). This user directory supports Address Group import, Recipient Validation and User Authentication if a password is provided.			
Directory Information			
Directory ID	LDB		
	Contains Password		
Search Addresses Which	contains 💌 Search		
Address Information			
bill.tobin@mycom.com	bill.tobin@mycom.com		
iane.cooper@surfcontro	ol.com		
Total Addresses 2	Current Page/Total Page - 1/1		
	Add Remove Back		

Figure 2 - 10 Local Database - Addresses

6 Click Add.



7 The Local Database - Add/Edit Address screen is displayed.

Local Database - A	\dd/Edit Address
This screen enables you Administrator's Guide for password is provided.	to configure a local DB user directory which can be used if you do not have an LDAP server (see the RiskFilter - E-mail more details). This user directory supports Address Group import, Recipient Validation and User Authentication if a
Address Information	
Address	
Password	
Confirm Password	
	Submit

Figure 2 - 11 Adding an address to the database

- 8 Enter the address that you want to add into the Address field.
- 9 If the database you are adding has a password then you need to enter this password into the Password field then confirm it. If the database does not have a password, you can leave these fields blank.
- 10 Click Submit.

SECURE PROXY

You can configure RiskFilter to act as a proxy server. In this setup, your users connect to the RiskFilter appliance rather than the mail server itself. The RiskFilter appliance collects the requested mail from the mail server and passes it back to the user. Using RiskFilter in this way provides an extra layer of security though you will need a POP3 server, Webmail or an IMAP proxy to do this. Your e-mail system can then be accessed remotely via the RiskFilter SSL VPN gateway.

To enable a proxy server:

1 Select General > Secure Proxy from the System Settings tab.

Secure Proxy Managemen		
This screen enables you to configurate	ate SurfControl RiskFilter POP3, Webmail and IMAP proxies. This can be used to give you secure nail using SurfControl RiskFilter SSI	
Total Simultaneous Connections	200	
Enable POP3 Proxy		
Incoming POP3 Port	110	
Back-end POP3 Server	Port 110 Require Secure Channel(SSL)	
Timeout 6	500 second(s)	
📃 Enable Webmail Proxy		
8 Incoming Webmail Port	so The port must be the same as the back-end webmail server port Require Secure Channel(SSL)	
Back-end Webmail Server T	Port 90 The port must be the same as the incoming webmail port Require Secure Channel(SSL)	
Timeout 6	600 second(s)	
Enable IMAP Proxy		
Incoming IMAP Port	143	
Back-end IMAP Server	Port 143 Require Secure Channel(GSL)	
Timeout 6	S00 second(s)	
	Submit Reset	

Figure 2 - 12 The Secure Proxy Setting screen



- 2 In the **Total Simultaneous Connections** field, enter the maximum number of connections that you want to be connected at any one time. The default setting is 200.
- 3 Select Enable POP3 Proxy.
- 4 Enter the following information:
 - Incoming POP3 Port The port number. The default port number is 110. Select the Require Secure Channel (SSL) option if required. It is not selected by default.
 - Back-end POP3 Server The IP address or domain name of the e-mail server required to act as your back-end proxy. In the Port field, enter the right port number. The default setting is 110. Select the Require Secure Channel (SSL) option if required.
 - **Timeout** The timeout period in seconds, the default value is 600 seconds.
- 5 Select Enable Webmail Proxy.
- 6 Enter the following information:
 - Incoming Webmail Port The port number. The default port number is 80. Select the Require Secure Channel (SSL) option if required.
 - **Back- end Webmail Server** The IP address or domain name of the e-mail server that is required to act as your back-end proxy.
 - **Port** The port number, the default port number is 80. Select the **Require Secure Channel (SSL)** option if required.
 - **Timeout** The time period for timeout in seconds. The default setting is 600 seconds.
- 7 Select Enable IMAP Proxy.
- 8 Enter the following information:
 - Incoming IMAP Port The port number, the default port number is 143. Select the **Require** Secure Channel (SSL) option if required.
 - Back-end IMAP Server The IP address or domain name of the e-mail server that is required to act as your back-end proxy.
 - **Port** The port number. The default port number is 143. Select the **Require Secure Channel** (SSL) option if required.
 - Timeout The time period for timeout in seconds, the default setting is 600 seconds.
- 9 After entering the above information, click **Submit** to save your settings. Click **Reset** to put all of the information back to its original state.



LOGS AND ARCHIVES

SurfControl RiskFilter stores messages that have been isolated. Initially these messages will be stored in the default directory. If you want RiskFilter to store messages in a different place, you must change the default directories within the Logs and Archives screen.

Logs and Archives		
This screen enables you to config usage of these directories and the directories.	ure where to store log files and archived messages. In addition, you can define the maximum disk number of days to retain entries. Use the Queue Manager to configure other message storage	
Log		
Directory to store log files	/home/rfbuilder/riskfilter/smg/data/log	
Days to keep log files	90 days (blank means no limit)	
Zip log files older than	days (blank means no compress)	
Keep maximum storage size at	512 MB and remove old ones on a FIFO basis (blank means no limit)	
Archived Message		
Archive level	None All messages except Spam mall Virus-infected message Instant decodes	
Directory to store archived	- Isolated message	
messages	/home/rfbuilder/riskfilter/smg/data/mailstore	
Days to keep messages	days (blank means no limit)	
Keep maximum storage size at	10240 MB and remove old ones on a FIFO basis (blank means no limit)	
	Submit Reset	

Figure 2 - 13 The Logs and Archives screen

Setting up the storage directories

You can set up directories to hold log files, spam messages etc. using the Directories screen.

To set up directories:

- 1 Select General > Directories from the System Settings tab.
- 2 Define how log files will be stored and how they will be treated when this happens:
 - **Directory to store log files** If you don't want to use the default location, enter the path to the required directory into this field.
 - **Days to keep log files** Leave this field blank to store log files indefinitely. If you enter a number into this field, the log file will be deleted after this length of time has passed.
 - **Zip log files older than...** Enter a number of days into the field then any log file that has been stored for this length of time will be zipped.



Caution: Zip files will be deleted along with any other log files, so you should move any zip files that you want to keep indefinitely out of this directory.

- Keep maximum storage size at ... MB and remove old ones on a FIFO basis specify that once the storage size of isolated messages reaches a certain size then the oldest will be deleted so the newest can be stored.
- 3 If there are no other directories that you want to set, click Submit.
- 4 The Archived messages directory enables you to specify where archived messages are stored.



- Archive level Define whether or not to archive files and what type of messages to archive if archiving takes place:
 - Select **None** for no archiving.
 - Select All messages except then select the relevant check boxes if you want to archive, but do not want to save this type of message.
- **Directory to store messages** Define where you want the archived messages to be stored by entering the path into the field.
- **Days to keep messages** Leave this field blank to store messages indefinitely. If you enter a number into this field, the log file will be deleted after this length of time has passed.
- Keep maximum storage size at ... MB and remove old ones on a FIFO basis Specify that
 once the storage size of isolated messages in the directory reaches a certain size then the oldest
 will be deleted so that the newest can be stored.
- 5 Once you have entered all of the details that you need, click **Submit**.

CERTIFICATE

For an extra layer of security RiskFilter supports the use of TLS verification. This helps prevent devices such as non-trusted routers from allowing a third party to monitor or alter the communications between server and client. It also enables SMTP agents to authenticate each others identities, should this be necessary. The RiskFilter server can receive messages transferred over TLS and can also send messages via this protocol to particular domains.

For TLS to work, the domains that will use this TLS authentication must be listed in the Domain-based Delivery screen. Certificates are managed in the **General > Certificate > Certificate Management** screen.

TLS Certificate Management							
This screen enables you to manage your TLS certificate. The Import Certificate operation enables you to import a signed certificate or keypair. The Export Certificate operation enables you to export your certificate, then import it onto another machine. The Export CSR operation enables you to export a Certificate Sign Request.							
Certificate							
Version	V1						
Signature Algorithm	MD5withRSA						
Serial Number	431d7286						
Issuer	www.surfcontrol.com, network security company, surfcontrol plc, beijing, beijing, CN						
Valid From	Tuesday, September 6, 2005 8:12:14 PM CST						
Valid To	Friday, September 4, 2015 8:12:14 PM CST						
Subject	www.surfcontrol.com, network security company, surfcontrol plc, beijing, beijing, CN						
	Import Certificate Export Certificate Export CSR						

Figure 2 - 14 The TLS Certificate Management screen

Notifications

When your certificate is due to expire, RiskFilter will send notifications until you import a new certificate. When you see these notifications you need to import a new certificate. They are sent in the following order:

- 30 days before the expiry date.
- Once every week after the first notification.
- · Every day during the last week before expiry.



Importing Certificates

A default certificate is supplied with RiskFilter but this will need to be renewed when it expires. The Import Certificate feature enables you add a new version to RiskFilter. You can also import a certificate that you have previously exported to a location on your network. or add a new certificate of your own. A custom certificate can be added as long as it is in one of the following formats:

- DER encoding certificate(binary) + private key; (keypair)
- DER encoding certificate(binary); (no private key)
- Base 64 encoding certificate (text) + base 64 encoding private key with PKCS8; (keypair)
- Base 64 encoding certificate (text); (no private key)
- Base 64 encoding certificate (text) + base 64 encoding private key with PKCS8 + ASN1; (keypair)

To import a certificate:

- 1 Select General > Certificate from the System Settings tab.
- 2 In the Certificate screen click Import Certificate.
- 3 An **Import Certificate File** dialog box will appear where you can either enter the path to your certificate or click **Browse** to navigate to it.
- 4 Once you have located your certificate click Import>>.

Exporting Certificates

It is a good idea to make a backup of the default certificate supplied with RiskFilter. This means that in the event of the certificate on the RiskFilter appliance being corrupted or destroyed, you can simply import your backup copy onto the machine. To do this you need to export your certificate to the network where you can store it in a location of your choice.

To export your certificate:

- 1 Select General > Certificate from the System Settings tab.
- 2 In the **Certificate** screen click **Export Certificate**.
- 3 A File Download dialog box will appear enabling you to save the certificate to your network.
- 4 Click **Save** and save the certificate into a location that can be accessed by the machine that you want to export it to.

Certificate Signing Request

You can export a CSR (Certificate Signing Request) for the default certificate. This contains the public key information which matches the private key installed on RiskFilter. The default directory for this key is: /opt/riskfilter/smg/conf/serverKeyStore.

If you are renewing your license you will need to export the CSR so that the updated license holds the same information.

To export the CSR:

- 1 Select General > Certificate from the System Settings tab.
- 2 In the Certificate screen click **Export CSR**.
- 3 A File Download dialog will appear enabling you to save the CSR to your network.
- 4 Click **Save** and save the CSR into the same location as the default certificate it should accompany.



RECEIVE SETTINGS

The Receive Settings menu contains all the sub-menus that are concerned with how mail is accepted before it is filtered. These settings specify how the mail should be treated when it is delivered to RiskFilter for processing.

CONNECTION CONTROL

Connection Control enables you to:

- · Limit the number of simultaneous connections made on your server.
- Enable or disable Real-Time Blacklist checking.
- Enable or disable reverse domain name lookup for IP addresses of incoming data.
- Allow specified IPs to bypass Real-Time Blacklist checking for data coming from specified IP addresses.

Use the Connection Control screen to enhance security.

Connection Control							
This screen enables you to control how connections are made to your server. Connection Settings limits the number of connections, either simultaneous or by a single IP address. Real- time black list checking enables you to determine if the sender of the message is black-listed, before the connection is established. SMTP Greeting Delay delays the initial response from the RiskFilter SMTP server and drops the connection when a client tries to send data before the SMTP server is ready. SMTP Greeting Delay is a countermeasure for many scripted SPAM agents which do not conform to SMTP standards.							
Co	nnection Settings						
Simu	ultaneous connections per IP	Allow up to 10	connections (Ma	aximum = 65535) *			
Simultaneous connections on each server		Allow up to 500	connections (Ma	aximum = 65535) *			
Time	eout	Disconnect connection	ns after 300	seconds of inactivity. *			
RB	L						
	Perform real-time black list (RBL) check						
	Real-time black list service provider						
	e.g., bl.spamcop.net; relays.ordb.org or l	Jackholes.mail-abuse.c	org. Separate mulf	tiple addresses with a semico	lon(;).		
	Perform reverse DNS lookup on every incoming connection (Note: SurfControl RiskFilter will drop the connection if reverse DNS fails to validate the host (this may significantly impact server performance).						
SM	SMTP Greeting Delay						
	Enable SMTP greeting message delay						
	Delay the SMTP greeting message to un	trusted clients for 3	seconds				
All	ow Access List						
IP or e.g., 10.1	nts with an IP in the Allow Access List will subnet address: 10.1.1.1 for single IP 1.0/24 for a block of IPs.	bypass SMTP Greeting	Delay and the rea	Add >> «< Remove			
							Cabinit (10001)

Figure 2 - 15 The Connection Control screen

Connection Settings

Use this section to improve system performance by limiting the number of simultaneous connections to the system.



RBL

Real-Time Blacklist (RBL) checking verifies the validity of message senders. If a sender is listed on an RBL, they will be prevented from sending messages to your internal MTA.

Reverse DNS enables you to make sure that e-mails sent to your RiskFilter server, are from legitimate domains. RiskFilter will stop them from sending e-mails to your internal MTA if reverse DNS fails (i.e. the sender is not from a legitimate domain). The default setting is not to perform a Real-Time blacklist (RBL) check so this function will need to be enabled if you want to use it.

RiskFilter will close the connection if reverse DNS lookup fails to validate the host. If you choose to enable Reverse DNS you must be aware that it may affect the performance of the RiskFilter server, causing legitimate users to be rejected. To obtain more RBL servers, visit: http://www.declude.com

SMTP Greeting Delay

You can specify that a SMTP greeting message is delayed for a specified time so that if a client tries to send data ahead of this time, the connection is dropped. This helps to prevent spam, as spam sending applications send a lot of messages very quickly. The connection is dropped as soon as a message is sent to the SMTP server before it is ready. This feature is disabled by default.

Allow Access List

Allow Access List enables you to specify an IP address or a group of IP addresses as trusted IP addresses. This enables them to bypass RBL checks and SMTP greetings.

To create an Access List:

- 1 Select Receive Settings > Connection Control from the System Settings tab.
- 2 Enter the maximum connections allowed per IP into the' Simultaneous connections per IP' field. The default setting is 100.
- 3 Enter the maximum number of connections allowed on the RiskFilter server into the **Simultaneous connections on each server** field. The default setting is 500.
- 4 Enter the maximum length of time for timeout in seconds into the **Timeout** field.
- 5 Select the **Perform real-time black list (RBL)** check check box. to enable RBL checking, then enter the network address of the blacklist provider into the **Real-Time black list service provider** field.
- 6 Select **Perform reverse DNS lookup on every incoming connection** to enable reverse DNS lookup.
- 7 Select the Enable SMTP greeting message delay check box.
- 8 Enter the number of seconds that you want the SMTP server to wait before it displays the SMTP greeting SMTP greeting, into the **Delay the SMTP greeting message to untrusted clients for _ seconds** field.
- 9 Enter the trusted IP address or IP address range into the IP or subnet address field.
- 10 Click **Add** to add an IP address or range to the address list on the right. If you want to delete an IP address or address range in the list, select the IP address or address range then click **Remove**.
- 11 Click **Submit** to put the new settings into effect or **Reset** if you want to cancel the modifications made to the current settings.

DIRECTORY ATTACK CONTROL

Directory Attack is used by questionable sources to gain access to internal e-mail accounts. A directory attack not only occupies large amounts of system resource but also, through the acquisition of e-mail accounts, creates spam problems for e-mail end users. RiskFilter enables you to control directory attack to limit the maximum messages and connections coming from an IP address over a given time period. Use the Directory Attack Control screen to configure this.

Directory Attack Control								
- This screen enables you to limit the maximum number of messages per IP address during different time periods. This will help to prevent Directory attacks								
	Limit the number of messages/connections per IP every	60 seconds 💌						
	Maximum number of messages:	30						
	Maximum number of connections:	30						
	Maximum number of same messages:	5						
	Limit the number of messages/connections per IP every	10 minutes 💌						
	Maximum number of messages:	90						
	Maximum number of connections:	90						
	Maximum number of same messages:	10						
	Drop connection							
	Maximum percentage of invalid addresses over the above thresholds:	50 %						
		Submit Reset						

Figure 2 - 16 The Directory Attack Control screen

There are two levels of control within this pane. The first enables you to specify in seconds how often the limit on messages is to be applied. The second will apply the same limits but in minutes. Specifying that messages are limited by the second gives you greater control than when you limit them by the minute.

To configure directory attack control:

- 1 Select Receive Settings > Directory Attack Control from the System Settings tab.
- 2 Select the Limit number of messages/connections per IP every ... seconds to enable the level 1 control then set the maximum number of messages, and connections. You can also set how often the same message is allowed to pass through RiskFilter.
- 3 Select the Limit number of messages/connections per IP every ... minutes to enable the level 2 control then set the maximum number of messages, and connections. You can also set how often the same message is allowed to pass through RiskFilter.
- 4 If you have selected one of the directory attack control options, you can select the **Drop Connection** option and set a percentage. Once the invalid messages/connections exceed this percentage of the total number of invalid messages/connections, the connection will be dropped automatically.
- 5 Click **Submit** to put the new settings into effect or **Reset** if you want to cancel the modifications made to the current settings.



RELAY CONTROL

RiskFilter enables you to stop your e-mail system from being used as an open relay by spammers. Relay control limits the server to only relaying e-mails for specific domains. Use the Relay Control screen to control relaying to and from your system.

Relay Control						
You can prevent an open relay by specifying the domains to be used as a relay by SurfControl RiskFiller.						
SPF Authentication Configuration						
Perform SPF checking against e-mail sender						
Accept e-mail for relay to the following domains						
domain e.g.,mydomain.com *.mydomain.com						
Accept a mail for relay from the following IP(s) Plate the following IP(s) will be use sometion control, jeller control, directory discle control and recipient validation. They will also bypass the data size measures after the competition and provide in decimited and the same liquids from measures accentrol.	te per connection, number of					
niessages per connection and number of ecupenis per message initia non message control/						
IP or submet address Add >> e.g., 10.1.1.1 for single IP << Remove 10.1.1.0/24 for a block of IPs. <						
Relay for internal senders						
O Authentication or trusted IP required						
Authentication or trusted IP not required but only allow relay to internal recipients Authentication or trusted IP not required and allow relay to any addresses * This online mixture internal long a comparison of the second sec						
mo upuuri myni reare a oeuniy iooue.	Submit Reset					

Figure 2 - 17 The Relay Control screen



Note: If you wish to define access to reports and logs by domain, you will first need to add these domains to this page.

SPF Authentication Configuration

You can ask E-mail Filter Appliance to check that messages are actually from a legitimate server. If enabled, this feature checks messages against the SPF record belonging to the sender and, if the server is not listed, the message will be rejected. This stops spammers forging messages that seem to be from the users themselves.

Controlling relaying of messages

Messages from IP addresses that have been added to the 'Accept e-mail for relay from the following IPs' list will be accepted for relay without any of the Connection Control, Relay Control, Message Control, Directory Attack Control or User Validation processes being performed on them.

To control relaying of messages:

- 1 Select Receive Settings > Relay Control from the System Settings tab.
- 2 Select the **Perform SPF checking against e-mail sender** check box if you want incoming message senders to be checked against an **SPF (Sender Policy Framework)** record. When SPF checking is selected RiskFilter will reject mail senders who fail to meet the SPF policy of the sending domain. Any other messages will be accepted, unless the following are selected:
 - **Reject mail from senders with no SPF records** When SPF checking finds that the senders domain does have an SPF record, reject the mail.

- **Reject mail from senders when SPF softfails** When SPF checking finds that the senders domain does not match the published SPF policy and ends with a SoftFail, reject the mail.
- **Reject mail from senders when there is an SPF error** When SPF checking finds that the senders domain has published an erroneous SPF record, reject the mail.



Note: These options appear when you select the Perform SPF checking against e-mail sender check box.

- 3 Enter the domain name you want to relay into the **domain** field.
 - Adding one domain e.g. mydomain.com will only accept messages from this domain.
 - Adding the domain with an asterisk e.g. *mydomain.com will accept messages from this domain and any sub-domains.
- 4 Click **Add>>**, the domain will be added to the list on the right. If you want to delete any domain from this list, select the domain then click **<<Remove** to delete it.

Allowing relaying to specific domains

You can configure E-mail Filter Appliance to only receive and relay messages that will be sent to specific domains. Messages sent to other domains will be rejected. You can add domains manually, or import lists of domains in a batch. These could be a list you have created and stored on the network or a list that you have previously exported from another appliance.

To manually add domains for relaying:

- 1 Enter the domain into the 'domain' text field.
- 2 Click Add. This will add the domain to the list. Click Remove to remove it.
- 3 Click Submit.

Importing lists of domains. You can import a list of domains to the appliance. This list must be a text file with the following properties:

- The charset must be UTF-8 if the files contains Chinese or Japanese characters.
- Each line is a domain name with leading and trailing spaces trimmed.
- · The domain name is case insensitive.
- When the file is scanned, an empty line is ignored.
- Lines starting with # or / are considered to be comments so are skipped.
- Invalid domains are ignored.

An example of this type of file would be:

sgyw.com cddn.net shkjm.com shhongtu.com #shshenyang.com


To import a list:

- 1 In the Relay Control screen, click Import.
- 2 In the dialog that follows, enter the path to the file or click Browse to navigate to it.
- 3 Click **OK**.

Exporting a list of domains. You can create a list of domains which can be exported, then imported on to another appliance. To do this:

- 1 In the Relay screen, click the **Export** button.
- 2 Specify where you want the text file to be stored.
- 3 Click OK.

RELAY FOR INTERNAL SENDERS

Specify the authentication needed when a user sends an e-mail from inside the domain:

- Authentication or trusted IP required When a sender is from the internal relay domain, the user must be authenticated or be sending messages from a trusted IP.
- Authentication or trusted IP not required but only allow relay to internal recipients When a sender is from the internal relay domain, Authentication or trusted IP is only required when sending to external domains.
- Authentication or trusted IP not required and allow relay to any addresses When a sender is from the internal relay domain, they can send to any domain even without being from a trusted IP. This will act as an open relay providing the user is from an internal domain.



Caution: Choosing the last option may leave your system open to security breaches.

RECIPIENT VALIDATION

The Recipient E-mail Address Validation screen enables you to improve the performance of the RiskFilter gateway system. Receivers' addresses are validated by user directories in order to prevent directory attack before inbound messages are received. Use the Recipient E-mail Address Validation screen to configure validation.

Recipient E-mail Ad	dress Validation			
Description	Lasa Validation	*		
Domain List				
Domain fayer.com		Add >> << Remove	lasa.surfcontrol.com surfcontrol.com	
User Directories				
Directory LASA Sendmail/ESMTP	v	Add >> << Remove	LASA Sendmail/ESMTP	
				Submit Reset

Figure 2 - 18 The Recipient E-mail Address Validation screen

Adding details of domains

In order to provide greater security, RiskFilter needs to check that the user comes from a valid domain. When you add a domain to the Recipient E-mail Address Validation screen, you first need to supply details of the domain. The domain List section enables you to do this.

Add validation servers

You must supply RiskFilter with a list of servers that are able to validate the user/s that you have added. Before you can do this you must create a connection with the server that will validate these users. Using this connection, e-mail messages are then checked to ensure that they belong to a domain and can be validated.

To add validation servers:

- 1 Select Receive Settings > Recipient Validation from the System Settings tab.
- 2 Click Add. The Recipient Email Address Validation screen is displayed.
- 3 In the **Description** field enter a description for this domain. This field is limited to 64 characters.
- 4 Select the domain that you need to be validated from the **Domain** list box.
- 5 Click **Add>>** to add it to the list. If you need to remove a domain from this list click the **<<Remove**.
- 6 Select the server that will supply validation from the **Server** list box.
- 7 Click **Submit** to put the new settings into effect or **Reset** if you want to cancel the modifications made to the current settings.



MESSAGE CONTROL

You can limit the message size, data size per connection, number of messages per connection, and the number of recipients per message. Use the Message Control screen to do this:

M	Message Control			
VVi pe	With this screen you can limit the message size, data size per connection, number of messages per connection, the number of recipients per message or the type of attachments contained in a message.			
	🛛 Limit message size			
	Maximum size	10240 (KB)		
	Limit data size per connection			
	Maximum data size	20480 (KB)		
	Limit number of messages per conne	ction		
	Maximum messages	20		
	Limit number of recipients per messa	ge		
	Maximum recipients	20		
	Block messages with attachments of a specific type			
	Attachment Extensions			
	Error Message	E-Mail Policy: Message contains an attachment ending with '		
		Submit Reset		

Figure 2 - 19 The Message Control screen



To configure message control:

- 1 Select **Receive Settings > Message Control** from the **System Settings** tab.
- Select Limit message size and enter a maximum message size into the corresponding Maximum 2 size (KB) field. This can prevent very large messages from using valuable bandwidth.
- 3 Select Limit data size per connection and enter a maximum amount of data into the corresponding Maximum data size (KB) field. This can help limit the receiving of messages with very large attachments, which can take up valuable bandwidth.
- Select Limit number of messages per connection and enter a maximum number of connections into 4 the Maximum messages field.
- Select Limit number of recipients per message and enter a maximum number of recipients into the 5 Maximum recipients field. This can save bandwidth by preventing one message from being sent to hundreds of users.
- 6 Select **Block messages with attachments of a specific type** if you never want to receive certain attachments.
 - Enter the attachment extension into the Attachment Extensions field. Multiple extensions must be separated by a semi-colon.
 - Enter a message into the Error Message field. This will be displayed to the MTA client when a message is blocked.
- 7 Click Submit to put the new settings into effect or click Reset if you want to cancel the modifications made to the current settings.

EXCEPTION CONTROL

While RiskFilter is processing messages, it may encounter unexpected exceptions, such as encrypted email messages. Exception Control enables you to specify what action is to be taken when exceptions occur:

- Deliver message Send the message to the recipient. This is the default action.
- Drop message Delete the message.
- Isolate message Send the message to the Isolate queue.

You can also specify that a message is sent when the Exception Control filter is triggered. Selecting this check box opens the screen up further so that you can enter details for this message.

Exception Control		
This screen enables you to spe as a result of abnormal situatio	acify the action to be taken whe ns, such as encrypted messa	an SurfControl RiskFilter is prevented from processing messages properly ges.
Condition	Filter Action	
When messages fail to be processed	Isolate message 🔽	To Queue quarantine 💌
Send Notification		
		Submit

Figure 2 - 20 Set what action is taken on messages



To configure exception control:

- 1 Select **Receive Settings > Exception Control** from the **System Settings** tab.
- 2 Choose a filter action from the When messages fail to be processed drop-down list box:
 - Deliver message Deliver the message to the intended recipient.
 - **Drop message** Delete the message without delivering it.
 - Isolate message Instead of delivering the message, send it to an specified folder and send a
 message to the intended recipient that the message could not be delivered. This is the default
 action.
- 3 Choose a **Queue** to send the message to, if the **Filter Action** is set to **Isolate message**.
- 4 Select the **Send Notification** check box if you want a message to be sent to the administrator when a filter is triggered. This will open up the screen so that you can enter information about the message.

Exception Control		
This screen enables you to spe as a result of abnormal situatio	ecify the action ons, such as e	to be taken when SurfControl RiskFilter is prevented from processing messages properly ncrypted messages.
Condition	Filter A	ction
When messages fail to be processed	Isolate m	nessage 💌 To Queue quarantine 💌
Send Notification		
	Sender	Original E-Mail Sender
		Administrator
		O User Specified
		stafford.home@shorne.surfcontrol.com
	To	Original E-Mail Sender
		Original E-Mail Receiver(s)
		Administrator
		User Specified
	Rubicat	Separate each entry with a semicolon(;)
	oubject	Caution: Invalid e-mail message format
Message Content		The message sent to %RCPTS% on %DATE&TIME%
		Sender: %SENDER% Message subject: %SUBJECT%
		● Do not attach message
		Attach modified message
		O Attach original message
		Submit Reset

Figure 2 - 21 The Exception Control screen

- 5 Select the option that corresponds to who you want to be listed as the sender of the notification:
 - **Original E-mail Sender** List the person who sent the original message as the sender of the notification.
 - Administrator List the administrator as the sender of the notification.
 - **User Specified** List the user whose e-mail address is in the field as the sender of the notification.
- 6 Select the option that corresponds to who you want the notification sent to:
 - Original E-mail Sender Send the notification to the person who sent the original message.
 - **Original E-mail Receiver** Send the notification to the person who was supposed to receive the original message.
 - Administrator Send the notification to the administrator.
 - **User Specified** Send the notification to the user whose e-mail address is in the field. You can add multiple users but each entry must be separated by a semi-colon.

- 7 Enter the subject that you want to be displayed when the notification is received, into the Subject field. For example: 'Caution: Invalid e-mail message format'.
- 8 Enter the message that you want to be displayed in the **Notification body** into the **Message Content** pane.
- 9 Specify what you want to do with the original message:
 - **Do not attach message** Send the notification without the original message.
 - Attach modified message Send a re-mimed version of the message with the return path removed.
 - Attach original message Send the notification with the original message in it's original format.
- 10 Click **Submit** to put the new settings into effect or **Reset** if you want to cancel the modifications made to the current settings.

BLACK LIST

Connections and messages will be refused if they come from addresses or domains, which are listed in the blacklist. The blacklist can be defined manually or imported from an address file. It can also be exported to a specified file. Use the Black List screen to configure your blacklist.

Black List			
This screen enables you to block messages ass from a text file of addresses. You can also export	ociated with certain IP, do the entire Black List to a te	main or e-mail addresses. You can e xt file.	enter this information manually or import i
Deny access for the following IPs		2 hosts	
IP or subnet address: e.g., 10.1.1.1 for single IP 10.1.1.024 for a block of IPs. Note: Hosts existing in Relay Control will not be blocked.	Add >> << Remove Import >> << Export	1,2,3,402 192,1,8,11/32	Begins With:
Deny access to the following domain and	e-mail addresses	0 addresses	
E-mail address: e.g. *@*.com (ail e-mails from .com) *@domain.com (ail e-mails from domain.com) john@domain.com (only from john@domain.com)	Add >> << Remove Impot >> << Export		Begins With: By Domain Names Look up
			Submit Reset

Figure 2 - 22 The Black List screen

Adding an IP or subnet address to the blacklist

You can block either a single IP or a block of IPs by using the Subnet Mask:

- Adding a single IP address such as 10.1.4.2 will deny messages from one IP address.
- Adding a block such as 10.1.4.0/24 will deny messages from a group of IP addresses.



Importing and exporting Lists

If you already have a list of IP addresses that you want to block you can import this list to your blacklist. Conversely once you have this list in your blacklist List (perhaps because you have been adding them dynamically on a regular basis) you can export this ready-made list of IP addresses to another appliance.

Adding domain or e-mail addresses to the blacklist

The blacklist enables you to deny access to specific domains or e-mail addresses. You can import/export lists of these domains and e-mail addresses to the blacklist in the same way as you import lists of IP addresses.

To create a blacklist:

- 1 Select Receive Settings > Black List from the System Settings tab.
- 2 Click Add>>. The IP address or subnet mask will appear in the list on the right. To remove an IP address or subnet mask select it in the list and click <<Remove. You can use the Lookup feature to find an IP address:</p>
- 3 Enter a number into the **Begins With:** field.



- 4 If you want to import or export a list click **Import** or **Export**. This will show an Explorer dialog box from which you can import or export the list.
- 5 Enter a path to the blacklist file or use **Browse** to navigate to the file.
- 6 Depending on what you are trying to do you will see either Import>> or Export>>:
 - Import>> You will now see the list of IP addresses in the right-hand pane.
 - Export>> You will be asked if you want to Save or Open the list.
 - Click **Open** to view the list in a text editor such as Notepad.
 - Click **Save** to save it to your system for use elsewhere.
- 7 Enter the domain or e-mail address, into the E-mail address field.
- 8 Click **Add>>**. The domain or e-mail address will appear in the list on the right. To remove a domain or e-mail address, select it in the list and click **<<Remove**. Use the Lookup feature to find an IP address:
 - Enter a number into the **Begins With:** field.
 - Click Look up.
- 9 Click **Submit** to put the new settings into effect or **Reset** if you want to cancel the modifications made to the current settings.



WHITE LIST

Messages will bypass Anti-Spam checking if they come from addresses or domains, which are listed in the White List. Use the White List screen to configure your White List.

White List			
With this screen you can allow m manually or import it from a text f the e-mails that have been recei	nessages associated with certain IP, domain or e-m file of addresses. You can also export the entire Whi ved.	ail addresses to bypass the Anti-Spa te List to a text file. Dynamic White Lis	m Agent. You can enter this information t automatically creates a White List based on
Allow access for the follo	wing IPs	0 hosts	
IP or subnet address: e.g., 10.1.1.1 for single IP 10.1.1.0/24 for a block of IPs.	Add >> < Remove import >> < Export		Begins With:
Allow access for the follo	wing domain and e-mail addresses	0 addresses	
Enter e-mail address: e.g. ⁻ @: com del e-mails form gadomain com (all e-mails for john@domain.com (only from)	Adg >> <- Remove m domain.com) Import >> ohn@domain.com) Export		Begins With: By Domain Names Look up
Dynamic White List			
Enable			Clear Dynamic White List
Occurrence			
Timeout	720 hour(s)		

Figure 2 - 23 The White List screen

Adding an IP or subnet address to the White List

You can block either a single IP or a block of IPs by using the Subnet Mask:

- Adding a single IP address such as 10.1.4.2 will allow messages from one IP address.
- Adding a block such as 10.1.4.0/24 will allow messages from a group of IP addresses.

Importing and exporting Lists

If you already have a list of IP addresses that you want to allow you can import this list to your White List. Conversely once you have this list in your White List (perhaps because you have been adding them dynamically on a regular basis), you can export this ready-made list of IP addresses to another appliance.

Dynamic White List

A Dynamic White List can be auto-generated based on the e-mail process information defined by RiskFilter. This ensures that normal messages can proceed to their destination directly, without any Anti-Spam policy checking being performed on them. This is done by setting an occurrence value which, when it is reached, will copy the address into the Dynamic White List automatically.

To set up a dynamic white list:

- 1 Select Receive Settings > White List from the System Settings tab.
- 2 In the **IP or subnet address** field, add a single IP address or a block of IP addresses. You can use the Lookup feature to find an IP address:
 - Enter a number into the **Begins With:** field.
 - Click Look up.
- 3 Click Add>>. The IP address or subnet mask will appear in the list on the right. To remove an IP address or subnet mask, select it in the list and click <<Remove. When you click Submit the counter



above the section will change to match the amount of IPs that you have added, and you will see text stating that the update was successful.

- 4 If you want to import or export a list click **Import** or **Export**. This will show an Explorer dialog box from which you can import or export the list.
- 5 Enter a path to the White List file or use **Browse** to navigate to the file.
- 6 Depending on what you are trying to do you will see either Import>> or Export>>:
 - **Import>>** You will now see the list of IP addresses in the right-hand pane.
 - **Export>>** You will be asked if you want to **Save** or **Open** the list.
 - Click **Open** to view the list in a text editor such as Notepad.
 - Click Save to save it to your system for use elsewhere.
- 7 Enter the domain or e-mail address, into the E-mail address field.
- 8 Click Add>>. The domain or e-mail address will appear in the list on the right. To remove a domain or e-mail address select it in the list and click <<Remove. When you click Submit, the counter above the section will change to match the amount of domains and e-mail addresses that you have added, and you will see text stating the update was successful.</p>
- 9 If you want to import or export an already existing list see steps 4 6 above.



SEND SETTINGS

The Send Settings menu provides sub-menus that enable you to specify how messages will be delivered when they are sent on to the user via RiskFilter E-mail.

DOMAIN-BASED DELIVERY

Domain-Based Delivery enables you to configure relay routing based on the domain of a recipient. It can also help you to configure the routing delivery methods for e-mail by resolving e-mail servers via DNS or forwarding to specified e-mail servers. If outgoing mail fails, RiskFilter will retry until a predefined limit is reached. Routing delivery is configured in the Domain-Based Delivery screen.

Domain-Based Delivery				
This screen enables you to specify the routing method for specific domains. You can configure DNS or Host-based e-mail forwarding to user-specified server(s). If more than one user-specified e-mail server is listed, SurfControl RiskFilter will deliver messages equally among these servers (so-called Round Robin). You can also enable TLS communication as well as ESMTP authentication for delivery to external and internal e-mail server(s). Another option is to go to Send Settings > Advanced Delivery to configure the retry settings in case of a delivery failure.				
Description	Delivery Method	Details		
In.com Delivery	Host-based e-mail forwarding	Edit		
Lasa Local SendMail	Host-based e-mail forwarding	Edit		
Default	DNS	Edit		
			Add Delete	

Figure 2 - 24 Existing routing methods for specific domains

Setting up the destination domains

To use Domain-based delivery, you need to add the domains of the destination servers to the Relay Control screen in RiskFilter. You can add multiple servers. If more than one user-specified e-mail server is listed, RiskFilter will control traffic automatically to ensure load balancing.

Delivering the messages

There are two ways of delivering a message:

- Resolve e-mail server via the following DNS server(s) Send messages to the internal SMTP server via a DNS server for resolution of host names.
- Forward e-mail to the following SMTP server(s) Send messages to the internal SMTP server directly so that it can deliver the message.

We recommend that you use Forward e-mail to the following SMTP server(s) for routing mail.



Using TLS authentication (Transport Layer Security)

If a message is sent via TLS then RiskFilter will be able to receive it, if STARTTLS Advertisement is enabled. However, if your mail server will only accept messages that are sent using TLS, then TLS must be enabled in RiskFilter in order for mail to be delivered to this server. See Certificate on page 25 for more information.

To set up domain-based delivery:

- 1 Select Send Settings > Domain-Based Delivery from the System Settings tab.
- 2 You will see the Default Routing Method that is supplied with the product.



Figure 2 - 25 The supplied Default Routing Method

- 3 Click Edit
- 4 Enter or edit the domain name in the **Description** field if necessary.
- 5 Select your domain from the **Domain** list box in the **Destination Domain Names** section.
- 6 Click Add>> to add the domain to the list on the right. If you need to remove a domain from this list click Remove>>.
- 7 Select Forward mail to the following SMTP server(s).
- 8 Enter the IP address of the SMTP server into the Server address field.
- 9 Enter the port number into the **Port** field. The default port number is 25.
- 10 Click Add>> to add the server to the list on the right.
- 11 RiskFilter supports the transferring of messages via the security protocol TLS. It will **always** RECEIVE messages sent by TLS transfer regardless of it's settings. However, if your mail server requires TLS authentication to DELIVER mail, then you must enable TLS mail delivery.

To enable TLS delivery, select My server(s) require communication over transport layer security.



Note: if your server does not require TLS for mail delivery, do NOT select this feature as this will stop settings from being submitted.

- 12 For more information on TLS see Certificate on page 25.
- 13 Select **My server(s) require authentication** if you want users to supply a username and password before they can access the server.
- 14 Enter a valid user name and password for authentication into the relevant fields.
- 15 Click **Submit** to put the new settings into effect or **Reset** if you want to cancel the modifications made to the current settings.

TRAFFIC CONTROL

After completing the security verification for mail, RiskFilter will forward it to the e-mail server according to the route configuration. To protect e-mail systems from the impact of heavy traffic, Traffic Control is designed to limit the mail traffic sent to the e-mail system. Use the Traffic Control screen to do this.

Fraffic Control	
This screen enables you to define the maximum number of messages SurfControl RiskFilter will relay to your in	ternal e-mail servers.
Maximum number of messages relayed to an internal e-mail server	
Note: Value 0 means no traffic control.	
	Submit Reset

Figure 2 - 26 The Traffic Control screen

To set up traffic control:

- 1 Select Send Settings > Traffic Control from the System Settings tab.
- 2 In the **Maximum number of messages relayed to an internal e-mail server** field, enter the maximum number of messages that you want to be relayed to your internal e-mail server per hour. This should be set up according to the incoming traffic setting of your e-mail server.
- 3 Click **Submit** to put the new settings into effect or **Reset** if you want to cancel the modifications made to the current settings.

ADVANCED DELIVERY

If a delivery attempt fails because the e-mail server reports a receiving error, RiskFilter places the message into the Deferred Messages queue. It then tries to deliver the message again according to specified rules. You can specify how long RiskFilter continues to make delivery attempts, the maximum retry period and the relevant actions to take after delivery has failed. Undeliverable messages are returned to the original sender or, if this cannot be done, a message is sent to the specified postmaster account. This is.accompanied by a copy of the original message. Use the Advanced Delivery screen to configure delivery attempts.

Advanced Delivery		
You can configure how lor period is reached, undeliv message will be delivered	g SurfControl RiskFilter will continue to make delivery attempts, and their frequency. When the maximum retry erable messages are bounced back to the original sender. If attempting to bounce a message fails, the to the specified postmaster e-mail account.	
Detrointensel		
Retry Interval	15 minute(s)	
Maximum retry period	1440 minute(s)	
Postmaster e-mail address		
	Submit Reset	

Figure 2 - 27 The Advanced Delivery screen

To configure Advanced Delivery:

1 Select Send Settings > Advanced Delivery from the System Settings tab.



- 2 Enter a time in minutes into the **Retry interval' field**. This specifies how long the server should wait before attempting to deliver the message again.
- 3 Enter a time in minutes into the **Maximum retry period** field. Once this period of time is reached the server will stop trying to send the message. Enter a time in minutes into the **Maximum retry period** field.
- 4 In the **Postmaster e-mail address field**, enter an e-mail address to receive the message after delivery has failed. When the maximum retry period is reached, and after attempting to send the message back to the original sender fails, RiskFilter will drop the message delivery and forward it to this specified e-mail account stating that the mail delivery failed. This will be accompanied by a copy of the original message.
- 5 Click **Submit** to put the new settings into effect or **Reset** if you want to cancel the modifications made to the current settings.



USER MANAGEMENT

Once you have completed the initial configuration of SurfControl RiskFilter there are other settings to implement that are vitally important to enable the product to work at its best. SurfControl recommends that you enhance RiskFilter's security in the following ways:

- Change the passwords to the Administrator accounts of the RiskFilter Console and RiskFilter Management Console.
- Set permissions for individual Administrators that will administer RiskFilter. In this way you can allow
 certain administrators to make departmental policy changes but stop them from administering the
 RiskFilter console itself.

There are two different accounts that are used to administer the RiskFilter appliance and they are both supplied with default passwords:

- **RiskFilter Console administrator account** The default password for this account is admin use the RiskFilter Console to change this.
- **RiskFilter System Management Console administrator account** The default password for this account is rfmngr use the RiskFilter Management Console to change this.

See **See "Launching SurfControl RiskFilter" on page 6** for more information on how to start each of these consoles.

ACCOUNT MANAGER

The Administrator Account Manager enables you to manage the accounts of anyone who has access to RiskFilter. It enables you to:

- Add new accounts by clicking Add.
- Delete redundant accounts by selecting the account and clicking Delete.
- · Edit existing accounts by clicking Edit alongside the account.

You can see these accounts in the Administrator Account Manager.



Figure 2 - 28 The Administrator Account Management screen



Changing the Administrator Account Password

SurfControl recommends that you change the supplied default passwords as soon as possible to enhance the security of the SurfControl RiskFilter appliance. The RiskFilter E-mail Console administrator account password is changed within the Admin Account Management screen.

To change the Administrator account password:

- 1 Log in to the RiskFilter console using the following details:
 - username = administrator
 - **password** = admin
- 2 Choose Account Manager from the User Management menu. The Administrator Account Management screen is displayed.
- 3 Click Edit.
- 4 Enter your new password into the Password field and confirm it.
- 5 Click **Submit**.

Specifying Administrator Access

Administrator Access can be useful to give certain people access to the RiskFilter appliance in order to carry out specific tasks such as making policy changes or managing messages stored in the various Queues.

The scope of the changes that these people can make will depend on the permissions that you set up for them. For example, you can allow certain individuals to make departmental policy changes, yet not allow them to administer the RiskFilter console itself. The Administrator Account Management screen is where you specify the type of access that you want your administrator/s to have.

Administrator Account Manager		
User Name	administrator	
Account Setup Time	05/15/2006	
First Name	Stafford	
Last Name	Home	
Password		
Confirm Password		
Description	Super Man In the Land of LASA	
Managed Modules	System Settings	
	Policy Manager	
	Reports & Logs	
	✓ Isolated Messages	
	Virus Messages	
	Spam Messages	
	Archived Messages	
	C Deferred Messages	
	Submit Reset	

Figure 2 - 29 The Administrator Account Manager screen



For each of the users you elect to carry out some of the administrative tasks within RiskFilter you need to:

- Create an account for each user (administrator).
- Add their appliance IP address as an authorized user. Once you have created an account for the
 administrator you can add the IP address of their machine to the RiskFilter console so that RiskFilter
 will recognize them as an authorized user. This will give you an extra level of security as, without it, the
 RiskFilter console will be accessible from anywhere.
- Select the parts of RiskFilter that they are allowed to manage. These tasks are divided into groups called Managed Modules. The following table contains an explanation of each module.

Module	What it does
System Settings	Enables the administrator to configure settings in the System Setting tab, as well as being able to view dash board and system report in the Reports and Logs tab.
Policy Manager	Enables the administrator to configure the settings in the Policy Manager tab.
Reports and Logs	Enables the administrator to configure the settings in the Report and Logs tab.
Isolated Messages	Enables the administrator to manage messages that have been isolated.
Virus Messages	Enables the administrator to manage messages that have been isolated because they contain a virus.
Spam Messages	Enables the administrator to manage messages that have been isolated because they are believed to be spam.
Archived Messages	Enables the administrator to manage messages that have been archived.
Deferred Messages	Enables the administrator to manage messages that have been deferred.

Table 1 Managed Modules

Setting up Administrator Access

To set up this administrator access you need to create an account for each administrator who will access the appliance.

To create an administrator account:

- 1 Select User Management > Account in the System Settings tab.
- 2 In the Administrator Account Manager screen click **Add**. Enter the following information:
 - User Name Enter the network username of the administrator.
 - Status Enable. You can choose Disable if you need to deny the administrator access to the RiskFilter console.
 - First/Last Name Enter the first and last name of the administrator.
 - Password/Confirm Password Enter a password for this administrator, and confirm it.
 - Description Enter a description that will help you to identify this administrator.
 - Managed Modules Select the modules that you want the administrator to have access to.
- 3 Click **Submit**.



- 4 Select Configuration from the General menu.
- 5 In the **Trusted IP(s)** field enter the IP addresses of all of the administrator's machines that you want to be able to access the RiskFilter appliance. If you enter more than one, then each IP address must be separated by a semicolon.
- 6 Click Submit.

Editing Administrator Accounts

To edit the account once you have set it up:

- 1 Select Account Manager from the User Management menu.
- 2 In the Administrator Account Manager screen click **Edit**. Change the relevant details in the Administrator Account Management screen.
- 3 Click Submit.

PERSONAL E-MAIL MANAGER

Personal E-mail Manager (PEM) enables the user to look at their isolated spam messages and lets them decide whether to delete the messages or treat them as legitimate e-mails. The RiskFilter console enables you set up the notification message that will be sent to users when they have isolated spam messages. PEM can be configured within the Personal E-mail Manager screen.

Personal E-mail Man	ager
This screen enables you to s They can also add specific s settings.	set up an e-mail for end-users containing a summary list of their isolated messages. Users can release individual messages that are reported in this summary enders to their own White List, so that future messages from these senders are not filtered for Spam. The end-user White List does not override any other global
Digest Notification Sch	edule
Max Messages	500
Digest Time(s)	100.00 01.00 02.00 03.00 04.00 05.00 06.00 07.00 08.00 09.00 110.00 11.00 12.00 13.00 14.00 15.00 16.00 17.00 18.00 19.00 20.00 21.00 22.00 23.00
Last Digest Time	Saturday, May 6, 2006 10:00:00 PM CST
Digest Message Templa	
operation	
Deep UDI	Always enforce end-user authentication
Base ORL	
Company	Suncontrol Personal E-mail Manager
Description	SurfControl RiskFilter- E-mail
Sender	postmaster@\$(domain)
Subject	SurfControl RiskFilter - you have isolated e-mails
Header	The following messages are isolated to \$(queue)
Footer	For more information contact your administrator.
Recipients List	
 All except the list below 	
Only the list below	
Enter recipient address: e.g. *@domain.com (all e-n john@domain.com (only joi	Add >> alis in domain.com) Import >>
	Submit Reset

Figure 2 - 30 The PEM screen



The PEM screen is composed of three sections:

- **Digest Notification Schedule** Set the time that a message will be sent to a user to inform them that they have spam messages waiting to be actioned.
- **Digest Message Template** Set up this message to the exact format that you require. This is the message that the user will see in their Inbox to tell them that they have spam waiting to be actioned.
- Recipients List Create a list of all of the users that you want to be able to use PEM.

For example: john@domain.com will apply only to this user while *@domain.com will apply to all users within domain.com



Note: Digest messages will only be sent to protected domains (those domains or addresses listed in Relay Control). Non-protected domains will not be able to receive digest messages.

Setting up the PEM message

The PEM screen enables you to define how and when you want messages to be automatically sent to users.

To set up PEM message:

- 1 Set a time for the message to be sent to users to tell them that they have spam messages waiting:
 - Max Messages Set how many linked messages are carried by each message. For example, if Max Messages is set to 50 and there are 150 messages waiting, three messages will be sent to the user (each carrying 50 messages and links) at the time specified in PEM Time. If Max Messages were set to 150, one message would be sent with all of the messages (and links) within it up to a maximum of 150 per message.
 - Digest Time(s) Select a time for the message to be sent to the users to say that they have messages waiting.
- 2 The PEM Message Template sets out the format for the messages that are sent to users when they need to manage their spam messages.
 - Operation Select one of the check boxes to indicate that the message is not spam. There are two options to choose from:
 - Report adds a button to the message that, when clicked will send the message to notspam@surfcontrol to indicate that this kind of message should not be classed as spam.
 - Deliver adds a button to the message that, when clicked, will deliver the message to the user without reporting it to SurfControl.
 - **Delete** delete the message without sending.
 - Always enforce end-user authentication when the user clicks the link to access their mail they will be asked to log in. Leaving this clear will allow them to check their mail without having to supply a user name and password.
 - **Base URL** This can be set so that it reflects the IP address of the RiskFilter appliance. If you are using a master/slave configuration, then this must be set to the URL of the master server.
 - **Company** This is the title of the message that the user receives informing them that they have spam messages waiting. You can change this default title by entering your own company details here.



- **Description** This lists the product that is filtering spam messages. You can change the default title by entering your own details here.
- **Sender** The default setting is postmaster@\$(domain). You can change this to something that more closely reflects your company set up, if necessary.



Note: You must enter the e-mail address in a valid format. This address might not even exist, but it must be in the correct form: XXXX@XXX.XXX, without any spaces.

- **Subject** As this will appear in the Inbox of the users e-mail client, it is a good idea to enter a title that will immediately draw their attention, e.g. 'You have isolated e-mail waiting'.
- Header You can replace the default The following messages are believed to be spam message with a message of your own.
- **Footer** You can change the default message so that it provides information on who to contact if they have a problem, for example the administrator's e-mail address or telephone number.
- 3 Once you have enabled PEM you can choose who has access to it by entering their details into the Recipients List section. There are two options in this section:
 - All except the list below Every user on the system will be able to use PEM and will receive messages unless their details are entered into the Enter recipient address: field. Select this option to change RiskFilter from the default setting. This way, if you have not added a list of users, everyone will still have access to this feature.
 - Only the list below Only the users listed in the Enter recipient address: field will receive messages and will be able to manage their own spam. With this option checked you MUST enter a list of users otherwise, even with PEM enabled, it will not work.
- 4 You can use wildcards to widen the range of addresses without having to enter them individually.
- 5 Once you have set up your message template click **Submit**. A message reflecting this style will now be sent to users when they have spam e-mail messages waiting.

SurfControl RiskFilter - you have isolated e-mails - Unicode (UTF-8)					
File Edit View Tools Message	Help				_
Reply Reply All Forward	Print Delete Previous Ne	Addresses			
From: stafford home@surfcontrol.com Date: 15 November 2005 11:00 To: icooper@lasa.surfcontrol.com Subject: SurfControl Riskiller - you have isolated e-mails					
	SurfControl Personal E-mail Manager				
			SurfCont	trol RiskFilter - E-mai	J
User: icooper@lasa.surfcontrol.con	<u>n</u>	Date: Tuesday, No	vember 1	5, 2005 7:00:00 PM CS	2
The following messages are believ	The following messages are believed to be spam Web Access				
Sender	Subject	Date	Size Op	peration	
ioe.spammer1@wayoutside.com Homeowners.Refi your home at 2005/11/15 18:57:42 1.7KB Delete Report Deliver					
Ioe.spammer1@wayoutside.com IlightimeUK Competitions 2005/11/15 18:57:43 6.2KB Delete Report Deliver Itewsletter - Win a D15,000 Ford Streetka					
For more information contact your administrator.					

Figure 2 - 31 What the user sees: Personal E-mail Manager



Adding users

You can add users or lists of users to PEM.

To add users:

- 1 Enter the user details of any user that you want to add to the **Recipients List** into the **Enter recipient** address: field.
- 2 Click **Add**. This will add them to the right-hand pane. If you want to remove any users from this list, select the user then click **Remove**.

Exporting lists of users

Lists of users can be exported for use with other features.

To export a list:

- 1 Select the list you want to export in the right-hand pane of the Recipients List section.
- 2 Click **Export**. You will be asked if you want to open the file or save it to your computer. Clicking **Open** will open the list in a text editor such as Notepad so that you can view it and print it if necessary.
- 3 Click **Save to** show a **Save As** dialog box where you can navigate to where you want to save the file.

Importing lists of users

You can import a list that you have created or have been sent. If you want to import a list you have created in RiskFilter (for example on another RiskFilter appliance) you must first export it to the network then import it onto the appliance that you want to add it to. Any user list that you want to import should be in a text file, with one address per line.

For detailed information on exporting then importing lists see **Importing and exporting Lists on page 69** for more information.

To import lists of users:

- 1 Click Import. An Import or Export Address File dialog box is displayed.
- 2 Click **Browse** and navigate to your saved text file containing your list of e-mail addresses. This could be a file created by exporting one of your own lists or a file that someone has supplied you with. The path to this file will appear in the field.
- 3 Click **Import**. You will now see the list of addresses in the right-hand pane.



END-USER CONTROL

Authorized users can log in to PEM with their own account and password, validated by a 'User Validation' connection and, depending on the settings in the Users List pane, can manage their own Black and White lists. To use PEM, a User Validation connection with 'Account Authentication' must be set up for End-Users to manage their own Black/White Lists.

Use the End User Control screen to set up End User Control.

End-User Control		
This screen enables the user to manage their own White List and Black List.		
End-user Bypass Anti-Spam Setting		
Enable end-users to bypass Anti-Spam checking		
Users List		
● Enable White List & Black List for all EXCEPT the addresses list below		
O Enable White List & Black List for ONLY the addresses list below		
Enter user e-mail address: e.g. *@domain.com (all e-mails in domain.com) john@domain.com (only john@domain.com)	Add >> << Remove import >> << Export	
		Submit Reset

Figure 2 - 32 The End-User Control screen

End-user Bypass Anti-Spam Setting

You can allow listed users to receive mail without an Anti-Spam check being run on them. If you have a user who must receive all messages, regardless of type, then this will prevent important messages being isolated as spam. It also can help where the type of mail a user receives results in a lot of false positives.

User List

You can specify users or lists of users then apply one of two conditions to them:

- Enable White List & Black List for all EXCEPT the address list below Everyone EXCEPT the users listed can manage their Black/White Lists.
- Enable White & Black List ONLY for the address list below ONLY the users listed can manage their Black/White Lists.

Setting up End User Control

To set up End User Control:

- 1 Select User Management > End-User Control from the System Settings tab.
- 2 Select Enable end-users to bypass Anti-Spam checking.
- 3 Decide who you want to apply the settings to and select the option that matches the way you want to apply the setting (see above).
- 4 In the **Enter user e-mail address:** field enter a domain or e-mail addresses in one of the following ways:
 - Enter the e-mail addresses of all users that you want to apply the settings to, e.g. user@mydomain.com
 - Enter *@ followed by the domain all users in that domain will be included in the list.

- 5 Click **Add**. The item will be added to the list on the right. If you want to delete a domain or e-mail address in the group, select the relevant address from the list and click **Remove**.
- 6 Click **Submit** to put the new settings into effect or **Reset** if you want to cancel the modifications made to the current settings.

USER AUTHENTICATION

There are two ways in which authentication is used:

- For authenticating PEM users Give users password protected access to the appliance, in order to manage their PEM account. This will not give them access to the RiskFilter Administrator.
- For authenticating remote users Authenticate users who send mail from the protected domain, from an IP address not listed in the Relay Control screen. These could include, for example, dial-up users. This will enable successful delivery of legitimate mail, while still denying e-mails from fraudulent addresses.

Authenticating PEM users

RiskFilter will authenticate users' accounts and passwords via user directories, before they log on to the PEM login page to check spam messages. Authentication is carried out in the User E-mail Account Authentication screen.

User E-mail Account Authentication				
User e-mail account authentication enables users to access their Personal E-mail Manager via a web interface.				
	Description	Details		
	Lasa Authentication	📥 Edit		
	Yamn Auth	📥 Edit		
	sendmail-UA	📥 Edit		
			Add Delete	

Figure 2 - 33 The User E-mail Account Authentication screen with existing accounts

RiskFilter enables end users to use a whitelist and a blacklist in order to manage their isolated spam messages.



Note: For more information on using PEM (originally called End User Spam Management), see Personal E-mail Manager on page 48.

To set up user authentication:

- 1 Select User Management > User Authentication from the System Settings tab.
- 2 Click Add.
- 3 Enter a name for the account into the **Description** field. This is limited to 64 characters.
- 4 Choose the domain that this user belongs to from the Domain list box.
- 5 Click **Add>>**. This will add it to the list pane on the right. To remove a domain, select it and click **<<Remove**.



- 6 Choose the server that will provide the authentication for this user from the 'Server' drop-down list.
- 7 Click Add>>. This will add it to the list pane on the right. To remove a server, select it and click <<Remove.
- 8 Click **Submit** to put the new settings into effect or **Reset** if you want to cancel the modifications made to the current settings.

Authenticating remote users

To authenticate remote users you first need to configure an LDAP connection and then add the user's domain to RiskFilter:

- 1 Configure an LDAP connection. See "User Directories" on page 13 for information on how to do this.
- 2 Select User Management > User Authentication from the System Settings tab.
- 3 Click Add.
- 4 Enter a name for the account into the **Description** field. This is limited to 64 characters.
- 5 Choose the domain that this user belongs to from the Domain list box.
- 6 Click Add>>. This will add it to the list pane on the right. To remove a domain, select it and click <<Remove.
- 7 Select the LDAP connection you have just created from the Directory drop down menu.
- 8 Click **Add>>**. This will add it to the list pane on the right. To remove a server, select it and click **<<Remove**.
- 9 Click **Submit** to put the new settings into effect or **Reset** if you want to cancel the modifications made to the current settings.



Note: Remote users will need to configure their mail clients to authenticate to the Riskfilter server when sending mail. They should use their email address as the username and their network password.



LICENSE & UPDATES

To ensure that RiskFilter is filtering at its optimum level you must update it regularly. This can either be a manual update which updates the product (and it's components) immediately, or you can specify a time and date for a regular (scheduled) update to take place.

UPDATE NOW

You can ask RiskFilter to update your Anti-Virus and Anti-Spam Agent definitions instantly in the Update Now screen.

Up	Update Now				
Upo	Update Now enables you to update the Anti-Virus and Anti-Spam Agents immediately.				
U	pdate Items Anti-Virus Agent definitions				
	Server	Engine Type	Latest Definitions	Last Update Attempt	Last Update Status
	Anti-Spam Agent definitions				
	Server	Content Type	Latest Definitions	Last Update Attempt	Last Update Status
	lasa.surfcontrol.com	Digital Fingerprints	08/07/2006 V3316	08/09/2006 01:33:42	Up to date
	lasa.surfcontrol.com	Heuristics	08/07/2006 V778	08/09/2006 01:33:41	Up to date
	lasa.surfcontrol.com	LexiRules	08/07/2006 V126	08/09/2006 01:33:40	Up to date
	lasa.surfcontrol.com	Internet Threat Database	08/08/2006 V1545	08/08/2006 17:34:08	Disabled
					Submit Reset

Figure 2 - 34 The Update Now screen

To update your Anti-Virus Definitions:

- 1 Select License & Updates > Update Now from the System Settings tab.
- 2 Click Anti-Virus Agent Definitions to expand the list. This screen shows details of:
 - Server The name of the server where the Anti-Virus Agent is installed.
 - Engine Type The Anti-Virus engine that this agent uses: e.g McAfee.
 - Latest Definitions The date and version number of the last definitions that were downloaded.
 - Last Update Attempt The last time an update was attempted.
 - Last Update Status How successful the update was:
 - **Up to date** the last update downloaded the most up to date database. There is no more recent database available.
 - Failed the update started but was disconnected or timed out.
 - Disabled there are no filters which use this database. Because of this, this update is disabled to conserve bandwidth.
 - Not Licensed there is no license available to update this database.
 - Waiting the update event is queued as only one update can be downloaded at one time.
- 3 **Updating** This database is currently attempting to update.
- 4 Select the check box alongside Anti-Virus Agent Definitions.
- 5 Click **Submit** to start the update.



Updating your Anti-Spam Agent Definitions

To update your Anti-Spam Agent definitions:

- 1 Select License & Updates > Update Now from the System Settings tab.
- 2 Click the Anti-Spam Agent Definitions link to expand the list. This screen shows details of:
 - Server The name of the server where the Anti-Spam Agent is installed.
 - **Content Type** The type of content filter that this Anti-Spam engine uses include:
 - Digital Fingerprints
 - Heuristics
 - LexiRules
 - Internet Threat Database
 - Latest Definitions The date and version number of the last definitions that were downloaded, if applicable. This is not shown for Internet Threat Database.
 - Last Update Attempt The last time an update was attempted.
 - Last Update Status How successful the update was:
 - Up to date the last update downloaded the most up to date database. There is no more recent database available.
 - Failed the update started but was disconnected or timed out.
 - Disabled there are no filters which use this database. Because of this, this update is disabled to conserve bandwidth.
 - Not Licensed there is no license available to update this database.
 - Waiting the update event is queued as only one update can be downloaded at one time.
 - Updating this database is currently attempting to update.
- 3 Select the check box alongside Anti-Spam Agent Definitions.
- 4 Click **Submit** to start the update.

AVA and ASA License Expired

As your Anti-Virus Agent and/or Anti-Spam Agent license approaches its expiry date a message will be sent reminding you to renew your license.



SCHEDULED UPDATE

It is important to schedule updates to the Anti-Spam and Anti-Virus agents so that you can be sure of the maximum protection. The Anti-Spam database is updated three times a day so the level of protection you are receiving can change rapidly on a day to day basis. Setting up these updates as an automatic event will ensure that your databases never run the risk of being out of date.

You can schedule updates in the Scheduled Update screen. Choose **License and Updates** then **Scheduled Update** in the System Settings tab. This will show you the Scheduled Update screen.

Scheduled Update		
Sheduled Updates enable you to have the Anti-Virus and Anti-Spam Agents updated automatically. If you have other content filtering components, these will also be updated.		
Schedule		
🗹 Anti-Virus Agent Update		
Repeat interval:	Every hour	
Day of week:	Sunday 🔽	
Time:		
🗹 Anti-Spam Agent Update		
Repeat interval:	Every hour	
Day of week:	Sunday 🛃	
Time:		
	Submit Reset	

Figure 2 - 35 The Scheduled Update screen

Use this screen to update the Anti-Virus and Anti-Spam Agents.

Updating the Anti-Virus Agent

To update the AntiVirus Agent:

- 1 Select the Anti-Virus Agent Update check box.
- 2 Specify how often the update is to occur by choosing an interval from the **Repeat Interval** list box. By default this is set to **Every hour**. We recommend that you keep this setting to ensure you receive updates as soon as they are ready.
- 3 If you set the repeat interval to **Every Week**, you need to specify the day of the week that you want the update to take place.
- 4 Specify the time of day that the update is to take place. For example:
 - Repeat interval = Every week
 - Day of week = Saturday
 - Time = 23:30

This will perform an online update of the Anti-Virus engine and definitions automatically, every Saturday at 11:30pm.

5 Click **Submit** to put these changes into effect.



Updating the Anti-Spam Agent

To update the Anti-Spam Agent:

- 1 Select the Anti-Spam Agent Update check box.
- 2 Specify how often the update is to occur by choosing an interval from the Repeat Interval list box. By default this is set to **Every hour**. We recommend that you keep this setting to ensure you receive updates as soon as they are ready.

If you set the repeat interval to **Every Week**, you need to specify the day of the week that you want the update to take place.

- 3 Specify the time of day that the update is to take place. For example:
 - Repeat interval = Every week
 - Day of week = Saturday
 - Time = 23:30

This will perform an online update of the Anti-Virus engine and definitions automatically, every Saturday at 11:30pm.

4 Click **Submit** to put these changes into effect.

LICENSE STATUS

You can check your licenses in the License Status screen.

License Status		
Туре	Status	View
General License	Valid	-View
Component License	Valid	-View
		Refresh

Figure 2 - 36 The License Status screen

Updating Component Licenses

In order to use the Anti-Spam and Anti-Virus Agents in your filters you need to have a valid license. Once you have registered these components you can check their status by looking at the Component License page.

Component License			
This license is used for component updates and operations. Use this screen to view your current license status or register a new license.			
Anti-Spam Agent Subscription Pro	perlies		
Subscription Type	Digital Fingerprint Updates		
Remaining Days	142		
Anti-Spam Agent Subscription Properties			
Subscription Type	Heuristic Updates		
Remaining Days	Remaining Days 142		
Anti-Spam Agent Subscription Properties			
Subscription Type	Subscription Type Lexirule Updates		
Remaining Days	142		

Figure 2 - 37 The Component License screen



Viewing component licenses

To view your component licenses:

- 1 Select License & Updates > License Status from the System Settings tab.
- 2 The License Status screen is displayed. You will see a list of licenses that are registered on this appliance. Click View by Component License to see all of the details of any licenses you have for these agents.

UPDATE SERVER

If you need to view the details of the server that updates your components (such as Anti-Virus and Anti-Spam agents), or even specify an alternative one, then you can do this in the Update Server Configuration screen.

Update Server	Update Server Configuration			
This screen enables you to manually set up your Update Server. You will need to do this if you use a proxy server to update RiskFilter - E-mail, or if you need to specify an alternative Update Server.				
Update Server D	letails			
Directory	/LiveUpdate/cgi-bin/liveupdateserver.			
Server	origin.listsrv.surfcontrol •			
Port	80 .			
Timeout	30000 *			
Proxy Server De	tails			
Server				
Port				
	Submit Reset			

Figure 2 - 38 The Update Server Configuration screen

The reason for this could be:

- You want to use a different update server to the default, to update your component licenses.
- You use a proxy server to access the Internet so any component updates will have to be carried out via this computer.

Manually setting up a license server

To manually set up your license server:

- 1 In the System Settings screen choose License & Updates > Update Server.
- 2 Enter the path to the update server into the **Directory** field.
- 3 Enter the name of the server into the **Server** field.
- 4 Enter the port number into the **Port** field. The default port number is 80.
- 5 Enter the path to the proxy server into the **Server** field.
- 6 Enter the proxy port number into the **Port** field.



Note: You can use the Configuration Wizard to add or amend license details by choosing **Help** > **Configuration Wizard** in the System Settings tab.



LICENSE SERVER

If you need to view the details of your license update server or specify an alternative one then you can do this in the License Server Configuration screen.

License Server (Configuration	
This screen enables you to manually set up your License Server. You will need to do this if you require a proxy server to update RiskFilter - E-mail, or if you need to specify an alternative License Server.		
License Server Details		
Server	http://register.surfcontrol.com/surfsoap/surfso	
Proxy Server Deta	ils	
Server		
Port		
	Submit Reset	

Figure 2 - 39 The License Server Configuration screen

The reason for this could be:

- · You want to use a different License Server to the default.
- You use a proxy server to access the Internet so any license updates will have to be carried out via this computer.



Note: You can use the Configuration Wizard to add or amend license details by choosing **Help** > **Configuration Wizard** in the System Settings tab.

Manually setting up a License server

To set up a license manually:

- 1 In the System Settings screen choose License & Updates > License Server.
- 2 Enter the path to the License server into the Server field.
- 3 Enter the path to the proxy server into the Server field.
- 4 Enter the port number into the **Port** field.
- 5 Click Submit.

User Number Exceeded

If the number of users exceeds that stipulated by your user license, you will be sent a message informing you of this fact. RiskFilter calculates the number of users by counting the number of successfully delivered e-mail messages over seven days.



Help

The Help menu gives you access to tools that can help you solve problems with RiskFilter E-mail.

ADMIN GUIDE

A direct link to this guide. Selecting this menu will launch this RiskFilter Administrator's Guide in pdf format.

CONTACT SUPPORT

You can fill in the Support screen and submit information to SurfControl Support so that they can help you with any aspect of the appliance that you are having difficulty with.

Contact Support	
This facility enables you to files.	send a problem description or question to SurfControl Technical Support along with the SurfControl RiskFilter diagnostic
Recipient	support@SurfControl.com
Sender's Address	stafford.home@surfcontrol.com
Sender's Name	
Organization	
Request Type	Suggestion 💌
Attach	 ✓ SurfControl RiskFilter configuration ✓ System information ✓ SurfControl RiskFilter latest log
Additional Information	
	Submit Reset

Figure 2 - 40 The Contact Support screen

Submitting a Support Request

To submit a Support Request:

- 1 Select Help > Contact Support from the System Settings tab
- 2 Ensure that the Recipient field contains the Support address: support @SurfControl.com
- 3 Enter your e-mail address into the Sender's Address field.
- 4 Enter your name into the **Sender's Name** field.
- 5 Enter the name of your organization into the **Organization** field.
- 6 User the **Request Type** drop-down list box to specify the type of request you are making and enter the relevant text into the Additional Information pane:
 - Suggestion Enter any ideas you have to improve RiskFilter.
 - Question Ask a general question about RiskFilter.
 - Feedback Enter feedback about a problem and whether it was fixed or not.
 - Problem Enter details of the problem and include relevant files as a diagnostic tool (see step 7).



- 7 Select the relevant check boxes from the **Attach** list to send configuration files to Support:
 - **Surfcontrol RiskFilter configuration** This gives a summary of the RiskFilter software configuration and includes:
 - RiskFilter E-Mail Version
 - Cluster Configuration
 - PEM Digest Configuration
 - System information This includes information useful for restoring the customers environment on Support machines and includes:
 - Policy Manger and Filter Settings
 - System Settings
 - User Authentication Settings
 - Connection Control Settings
 - SurfControl RiskFilter latest log This attaches the latest activity log from RiskFilter.
- 8 Fill in the 'Additional Information' pane with your request (see Step 6).
- 9 Click Submit.

FIRSTBOOT WIZARD

The FirstBoot wizard enables you to set up how the RiskFilter appliance is configured within your system using a wizard. See the *Starter Guide* for more details.

CONFIGURATION WIZARD

The Configuration wizard enables you to set up how the RiskFilter software is configured within your system using a wizard. See the *Starter Guide* for more details.



KEY POINTS

The following list is a summary of the main points covered in Chapter 2. Use this list as a quick reminder of what you can do within the System Settings tab:

- RiskFilter can notify the administrator by sending a message to a predefined address, when an event such as a service stopping occurs.
- User Directories provide RiskFilter with recipient address validation and end-user authentication. Servers that can be used are: Microsoft Active Directory, IBM LDAP Server, Generic LDAP, ESMTP, Recipient File and Local Database.
- Microsoft Active Directory, IBM LDAP Server, Generic LDAP, ESMTP and Local Database can all be used for PEM authentication.
- A user-defined list of e-mail addresses and passwords can be imported onto the RiskFilter appliance and stored in the database for authentication and validation purposes.
- You can configure RiskFilter to act as a proxy server for POP3, Webmail and IMAP.
- You can store messages in a different place to the default by changing the default directories within the Logs and Archives screen.
- For an extra layer of security RiskFilter supports the use of TLS verification/encryption.
- If your certificate is due to expire, RiskFilter will notify you of the fact. When you see these notifications
 you need to import a new certificate.
- A default certificate is supplied with RiskFilter but this will need to be renewed when it expires, or replaced with a certificate from a certificate authority such as Verisign.
- It is a good idea to make a backup of the default certificate supplied with RiskFilter. This means that in the event of the certificate on the RiskFilter appliance being corrupted or destroyed, you can simply import your backup copy onto the machine.
- Improve system performance by limiting the number of simultaneous connections to the system.
- You can specify that a SMTP greeting message is delayed for a specified time, so that if a client tries to send data ahead of this time, the connection is dropped. This helps to prevent spam, as spam sending applications send a lot of messages very quickly.
- You can specify an IP address or a group of IP addresses as trusted IP addresses, to enable them to bypass RBL checks and SMTP greeting.
- RiskFilter enables you to stop your e-mail system from being used as an open relay by spammers. Relay control limits the server to only relaying e-mails for specific domains.
- You can limit the message size, data size per connection, number of messages per connection, and the number of recipients per message.
- A message can be sent to the administrator when a filter is triggered.
- Connections and messages will be refused if they come from addresses or domains which are listed in the blacklist.



- You can block either a single IP or a block of IPs by using the Subnet Mask.
- If you already have a list of IP addresses that you want to block, you can import this list to your blacklist.
- A Dynamic White List can be auto-generated based on the e-mail process information defined by RiskFilter. This ensures that normal messages can proceed to their destination directly, without any Anti-Spam policy checking being performed on them.
- Domain-Based Delivery enables you to configure relay routing based on the domain of a recipient. It can also help you to configure the routing delivery methods for e-mail by resolving e-mail servers via DNS or forwarding to specified e-mail servers.
- If a message is sent via TLS then RiskFilter will be able to receive it. However, if your mail server will only accept messages that are sent using TLS, then TLS must be enabled in RiskFilter in order for mail to be delivered to this server.
- Traffic Control is designed to limit the mail traffic sent to the e-mail system to protect e-mail systems from the impact of heavy traffic.
- If a delivery attempt fails because the e-mail server reports a receiving error, RiskFilter places the message into the Deferred Messages queue.
- Administrator Access can be useful to give certain people access to the RiskFilter appliance in order to carry out specific tasks such as making policy changes, or managing messages stored in the various Queues.
- If you enter more than one trusted IP address, then each IP address must be separated by a semicolon(;).
- Personal E-mail Manager (PEM) enables the user to look at their isolated spam messages and lets them decide whether to delete the messages or treat them as legitimate e-mails.
- You can use wildcards to widen the range of PEM user addresses without having to enter them individually.
- You can allow listed users to receive mail without an Anti-Spam check being run on them.
- You must update components such as Anti-Spam Agent and Anti-Virus Agent regularly, to ensure that RiskFilter is filtering at its optimum level.
- The Anti-Spam database is updated three times a day, so the level of protection you are receiving can change rapidly on a day to day basis.
- If the number of users exceeds that stipulated by your user license, you will be sent a message informing you of this fact.

Policy Manager

۲he Policy Manager tab	bage 66
Creating a Policy	bage 67
Address Group	bage 69
Queue Manager	bage 71
Dictionary Manager	bage 73
Global Policy	bage 79
Key Points	ige 103



THE POLICY MANAGER TAB

This chapter explains how to use the Policy Manager tab to configure anything to do with the management of e-mail messages that pass through RiskFilter. By controlling who has policies applied to them and what these policies actually do, you can fine-tune your filtering to exactly match your company's needs.

TERMINOLOGY USED

The following terminology is used in this chapter:

- DFP (Digital Fingerprint) Compares mail messages to known spam from different categories.
- Heuristics Uses regular expressions to determine the likelihood that an e-mail message is actually Spam.
- LexiRules Analyses words, phrases and patterns commonly found in spam to identify e-mail messages as possible spam.

WHAT CAN BE CONFIGURED IN THE POLICY MANAGER TAB?

The Policy Manager tab is where you set up your filtering policies. You can use the ready-made filters supplied with the product or you can create your own filters.



Figure 3 - 1 The Policy Manager tab

Policy Manager enables you to:

- · Add and remove groups of users and addresses.
- · Create and manage queues for isolated e-mails to be stored in.
- Set up dictionaries that enable RiskFilter to search for specific words in a message.
- Configure global policies that apply to everyone.



CREATING A POLICY

There are three steps to creating a policy:

Step 1 - Defining users – Add the users, and groups of users, that you want to filter.

Step 2 - Defining actions – Define what should be done with a message that triggers a filter.

Step 3 - **Defining the rules** – Create filters to find messages of a specific type. You can filter virus/spam messages by adding one or more types of filter to the policy.



Note: RiskFilter supports multi-layered policies: global policy and sub-policy. If a filter is writable, it can be overwritten by a sub-policy (its child or grandchild). A read-only policy cannot be overwritten by a sub-policy.

STEP 1 - DEFINING USERS

RiskFilter enables you to apply different filtering solutions to messages from specific address groups, according to different routing paths. There are three ways to add an e-mail address:

- · Add the address/es manually
- · Import the address/es from a file
- · Import the address/es from an LDAP connection

See Address Group on page 69 for more details on how to add addresses.

STEP 2 - DEFINING THE ACTION

Filter action determines how the message is finally processed. RiskFilter scans the messages and their attachments then takes action according to the settings in the different filters. The action is set when you create a new filter, within that filter's configuration screen.

Action if filter triggered	
Modify Subject	
X-Header	
🗌 Сору То	
Save to	junkmail 💌
Send Notification	junkmail guarantine
🔿 Deliver Message	DEAD
💿 Drop Message	Exception

Figure 3 - 2 The Action if filter triggered section

These actions include:

- Modify Subject Modify the original subject, by adding specific content in front of the original subject.
- X Header Add a specified X-Header to all messages which triggered the filter.
- **Copy to** Send a copy of the original message to a specified e-mail account. This would generally be the e-mail system administrator, the recipient will have no knowledge of this action.


- Save to Isolate Message Send the message to the isolated message store for further processing.
- Save to Spam Message: Send the message stopped by an Anti-Spam filter to the Spam Message store for further processing.
- Save to Virus Message Send the message stopped by an Anti-Virus filter to the Virus message store for further processing.
- Send Notification Sends a pre-defined notification to specified recipients including a copy of the email message that triggered the filter.
- Deliver Message Deliver the message.
- Drop Message Delete the message without delivery.

See Address Group on page 69 for details on how to manage these queues.

STEP 3 - DEFINING THE RULES

Once you have defined who you want to apply policies to, plus the actions that should be taken when messages trigger filters applying to these users, you need to create the rules. Rules are defined by creating filters that set the contraints, and action to be taken, on messages that trigger one of these filters.

All messages passing through SurfControl RiskFilter - E-mail will be checked against the Global Policy filters. By default, sub-policies inherit filters from their parent policies. Sub-policies can also overwrite their parent filters to meet their own specific needs.

Jobal Policy Filter List						
	Index	Order	Name	Origin	Туре	Status
	1	₫	Anti-Virus Agent - ClamAV	Global Policy	Anti-Virus Agent - ClamAV	disable / read-only
	2	រីរូ ប្អ	Anti-Spam Agent - DFP	Global Policy	Anti-Spam Agent - DFP	enable / read-only
	3	₫ ₿	<u>Anti-Spam Agent -</u> <u>Heuristics</u>	Global Policy	Anti-Spam Agent - Heuristics	enable / read-only
	4	រ៉ី ប៉ូ	Anti-Virus Agent - McAfee	Global Policy	Anti-Virus Agent - McAfee	enable / read-only
	5	₫ ₿	<u>Anti-Spam Agent -</u> LexiRules	Global Policy	Anti-Spam Agent - LexiRules	enable / writable
	6	₿ \$	Internet Threat Database	Global Policy	Internet Threat Database Filter	enable / writable
	7	រុំ 🕯	Standard Disclaimer	Global Policy	Standard Disclaimer	enable / read-only
	8	រ៉ី ប៉ិ	HTML Crash?	Global Policy	Advanced Content Filter	enable / writable
	9	Ŷ	<u>Kill test</u>	Global Policy	Content Guardian	enable / writable
						Add Del

Figure 3 - 3 The Global Policy Filter List

See Global Policy on page 79 for details on how to create and configure filters.



Address Group

You can add one or more address group(s) to the address group list, and each address group can include a group of e-mail address lists. Addresses are added using the Address Group screen.

Address Group		
Define the group e-mail addresses.		
Address group		
Name		
E-mail address e.g. *@*.com (all e-mails from .com) *@domain.com (all e-mails from domain.com) john@domain.com (only from john@domain.com)	Add >> << Remove Import >> << Export	
		Submit Reset

Figure 3 - 4 The Address Group screen

IMPORTING AND EXPORTING LISTS

If you already have a list of domain or e-mail addresses to apply your policy to, you can import this list into Policy Manager and use it in your policy. You can also export a list of IP addresses to another appliance.

To add addresses to Policy Manager:

1 Choose Address Group from the Policy Manager tab menu.

Address Group				
An aduress group is used to identify a group of individuals that policies Will be applied to, it contains a set of e-mail addresses.				
	1	High (Disable ASA)	Not in use	
	2	High (Disable AVA)	Not in use	
	3	Medium (Alert Only)	Not in use	
			Add Delete	



- 2 Click Add. The Address Group page is displayed (See Figure 3 4).
- 3 Enter the address group name that you want to define (such as in.com) into the **Name** field.
- 4 In the **E-mail address** field, enter the e-mail address(s) that will form the group.
- 5 In the Enter user e-mail address: field enter domain or e-mail addresses in one of the following ways:
 - Enter the e-mail addresses of all users that you want to apply the settings to e.g. john@mydomain.com



- Enter *@ followed by the domain to have all users in that domain included in the list e.g.*@mydomain.com
- Enter *@* to have all users included in the list regardless of their domain e.g.*@*.com
- 6 Click **Add**, the item will be added to the list on the right. To delete an e-mail address in the group, select the relevant address from the list on the right and click **Remove**.
- 7 If you want to import or export a list, click **Import** or **Export**. This will show an Explorer dialog box.
- 8 Enter a path to the blacklist file or use **Browse** to navigate to the file. The path to this file will then appear in the field.
- 9 Depending on what you are trying to do, you will see either Import>> or Export>>:
 - **Import>>** There are two types of file import available:
 - Import from file click Browse and navigate to your saved text file containing your list of e-mail addresses. This could be a file created by exporting one of your own lists or a file that someone has supplied you with. The path to this file will appear in the field.
 - Import from an LDAP server choose the directory name of an LDAP server that includes the e-mail addresses to be imported from the drop-down list. You must have a LDAP connection configured before you can do this. You will now see the list of IP addresses in the right-hand pane.
 - **Export>>** You will be asked if you want to **Save** or **Open** the list.
 - Click **Open** to view the list in a text editor such as Notepad.
 - Click **Save** to save it to your system for use elsewhere.
- 10 Click Submit to save your settings or click Reset to cancel changes made to the current settings.

DELETING ADDRESS GROUPS

You can delete address groups that you no longer require.

To delete addresses:

- 1 In the **Address Group** screen, select the check box for the address group that you want to remove.
- 2 Click **Delete**. This will remove the selected address group.



QUEUE MANAGER

When a message triggers a filter it can be sent to a queue, where it can be stored until you are ready to deal with it. Queue Manager enables you to manage the three supplied queues as well as any queue that you create. The default queues are:

- Virus mail This stores messages that have triggered the Anti-Virus filter.
- Junk mail This stores messages that have triggered the Anti-Spam filter.
- Quarantine This stores messages that need to isolated, but which haven't triggered the Anti-Virus or Anti-Spam filter.

These queues can be configured in the Queue Manager screen.

Queue Manager						
This screen enables you to manage RiskFilter - E-mail's queues. There are three pre-configured default queues: junkmail (for spam messages), virusmail (for virus infected messages) and quarantine (the default isolation queue for non-spam and non-virus filters). This screen can also be used to create user-defined queues which are useful for saving specific mail types to their own queue. To view the contents of the queues, see Spam Messages, Virus Messages and Isolated Messages in the Reports & Logs section.						
Queue Name	Description	In Use	Edit			
virusmail	Virus Messages	In use	📥 Edit			
junkmail	Spam Messages	In use	📥 Edit			
quarantine	Isolated Messages	In use	📥 Edit			
			Add Delete			

Figure 3 - 6 The Queue Manager screen

ADDING QUEUES

You can create your own custom queues where messages that have been stopped can be stored. You could, for example, have separate queues for different virus engines or a queue for messages that need to be stopped and checked before delivery. Queues are created in the Queue Manager Screen.

Queue Manager				
Create Queue				
Queue Name	A Only English letters (a-z) and digits (0-9) are allowed			
Description				
	Enable the sending of a digest message, and end-user e-mail management			
Store messages in /home/rfbu	ilder/riskfilter/smg/data/mailstore			
Keep message for 30	days (blank means no limit)			
Keep maximum storage size at	1024 MB and remove old messages on a FIFO basis (blank means no limit)			
	Submit Reset			

Figure 3 - 7 Creating a new Queue

After you have submitted your changes the new queue will appear in the **Save to** list box in the Actions if Filter Triggered section.



To add a Queue:

- 1 Select Queue Manager from the Policy Manager tab.
- 2 Click Add in the Queue Manager screen.
- 3 Enter a name for the Queue into the **Queue Name** field.
- 4 Enter a description of the Queue into the **Description** field.
- 5 Select **Enable sending digest message and end user e-mail management** if you want to use this feature. In the **Directory to store messages** field, enter the path to the new queue.
- 6 Specify how long you want messages in this queue to be kept before they are deleted, in the Days to keep messages days (blank means no limit) field. If you do not enter a value in this field, messages will be kept indefinitely.
- 7 Specify how the size in MBs that the queue will be allowed to reach before messages will start to be deleted, in the Keep maximum storage size at MB and remove old ones on a FIFO basis (blank means no limit) field. Once this value is reached, the oldest message in the queue will be deleted to make space for the newest. This will be a continuous process.
- 8 Click **Submit** to save these new settings.

Editing a Queue

Once you have created a queue you can edit it at any time.

To edit a queue:

- 1 In the **Policy Manager** tab click **Queue Manager** in the left-hand menu.
- 2 In the Queue Manager screen, click **Edit** alongside the queue you want to edit.
- 3 Make changes to the settings within the **Update Queue** screen.
- 4 Click **Submit** to save these new settings.



DICTIONARY MANAGER

You can use the supplied SurfControl dictionaries or create your own using the Dictionary Manager. These then be used for the following:

- Setting a threshold for a word within the Dictionary Threshold Filter for tracking how many times a particular word appears in a message.
- Using dictionaries to select words for the Expression List in the Advanced Content Filter.

SURFCONTROL DICTIONARIES

The SurfControl dictionaries are provided with the RiskFilter appliance. They cover the same type of content as the categories found within the Internet Threat Database. You can import or export dictionaries, particularly dictionary packs that are available from www.surfcontrol.com.

Editing SurfControl Dictionary properties

You can change the name, add messages and set the language of any of the SurfControl dictionaries.

To edit a dictionary:

- 1 Select Dictionary Manager > SurfControl Dictionaries from the Policy Manager tab.
- 2 Click the title of the dictionary that you are interested in.
- 3 To change the name of the dictionary, enter a new name into the Dictionary Name field.
- 4 To give a brief summary of the dictionary contents, enter relevant words into the **Comment** field.
- 5 To add a message, enter a message into the **Open Message** pane and check the **Display this message when dictionary launches**. The picture shows one of these messages created for the Adult dictionary which appears when you click the Adult link to view the dictionary contents:

Microsoft Internet Explorer		
♪	Warning! This dictionary contains offensive information.	
	ОК	

6 To change the Language of the dictionary, select the required language from the Language list. The following screen shot shows the Dictionary Properties for the Adult Dictionary. The text entered into the Open Message pane will appear in the warning dialog box in Step 5.

Dictionary Properties		
Dictionary Name	Adult	
Comment	Sexually Explicit, Adult-Oriented	
Open Message	Warning! This dictionary contains offensive information.	
	☑ Display this message when dictionary launches	
Language	English	

Figure 3 - 8 Setting Dictionary Properties

- 7 See the following procedures for information of further changes that can be made to the SurfControl dictionaries.
- 8 Click **Submit** to save these new settings.



Changing the value of words in the SurfControl Dictionaries

You can change the value of a word or phrase to fine-tune your filtering. You may want to do this for the following reasons:

- You find that messages containing a certain word are not being stopped. Increasing the value will mean that any messages containing this word will need to have fewer occurances before the filter triggers.
- You find that messages containing a certain word are being stopped unnecessarily. Decreasing the value will allow more occurances of the word within a message before the filter is triggered.

To change the value of words and phrases:

- 1 Select **Dictionary Manager > SurfControl Dictionaries** from the **Policy Manager** tab.
- 2 Click the title of the dictionary that you are interested in.
- 3 Click the word or phrase that you want to change the value for.
- 4 In the **Add/Edit Phrase** screen you will see the settings for the selected word or phrase. Change the value in the **Phrase Value:** field.

Add/Edit Phrase				
Properties				
Word or Phrase				
Phrase Value	0			
			Submit Cancel	

Figure 3 - 9 Add a Word or Phrase or Phrase Value

- · Increasing the value will increase filtering strength
- Decreasing the value will decrease filtering strength
- 5 Click **Submit**. The new value will be seen in the dictionary list alongside the word it is attached to.
- 6 Click **Submit** to save these new settings.

Adding words to the SurfControl Dictionaries

If you find that a useful word or phrase is missing from one of the SurfControl Dictionaries you can add it yourself. This saves creating a new custom dictionary simply to hold this word or phrase.

To add a word or phrase:

- 1 Select Dictionary Manager > SurfControl Dictionaries from the Policy Manager tab.
- 2 Click the title of the dictionary that you are interested in.
- 3 Click **Add**.
- 4 Enter the word or phrase you want to add into the **Word or Phrase** field.
- 5 Enter a phrase value into the **Phrase Value** field.
- 6 Click Submit. The new word or phrase will be seen in the dictionary list.
- 7 Click Submit to save these new settings.

Deleting a word or phrase

You can remove any word or phrase from the dictionary.



To remove a word or phrase:

- 1 Select **Dictionary Manager > SurfControl Dictionaries** from the **Policy Manager** tab.
- 2 Click the title of the dictionary that you are interested in.
- 3 Select the check box alongside the word or phrase that you want to remove.



Note: Selecting the check box alongside a dictionary, rather than one of the words within it, then clicking **Delete** will delete the whole dictionary. Only do this if you are sure you want to delete the whole dictionary.

4 Click **Delete**.

5 Click **Submit** to save these new settings.

CUSTOM DICTIONARIES

You can create a dictionary that fits your needs exactly, giving you a shortcut to words that you know are particularly applicable to the type of filtering that you need.

Create a new dictionary

When you create a new dictionary, you first have to create the dictionary then add words and phrases to it. These words and phrases must then have a value assigned to them so that the Dictionary Threshold filter can use them.

To create a new dictionary:

- 1 Select **Dictionary Manager > Custom Dictionary** from the **Policy Manager** tab.
- 2 Click Add.
- 3 Enter a new name for the dictionary into the **Dictionary Name** field.
- 4 Enter words to give a brief summary of the dictionary contents into the **Comment** field.
- 5 Add a message to the **Open Message** pane and select **Display this message when dictionary launches** check box. The picture shows a message created for the adult dictionary which appears when you click the Adult link to view the dictionary contents.

Microso	Microsoft Internet Explorer		
♪	Warning! This dictionary contains offensive information.		
	ОК		

6 Select the Language for the dictionary by selecting the required language from the Language list. The following picture shows the Dictionary Properties for the Adult Dictionary: The text entered into the Open Message pane will appear in the warning dialog box in Step 5.

Dictionary Properties		
Dictionary Name	Adult	
Comment	Sexually Explicit, Adult-Oriented	
Open Message	Warning! This dictionary contains offensive information.	
	Display this message when dictionary launches	
Language	English	

Figure 3 - 10 Dictionary Properties



- 7 Click Add.
- 8 Enter the word or phrase you want to add into the **Word or Phrase** field.
- 9 Enter a phrase value into the **Phrase Value** field.

Add/Edit Phrase				
Properties				
Word or Phrase				
Phrase Value	0			
	Subm	it Cancel		

Figure 3 - 11 Add a Word or Phrase or Phrase Value

- 10 Repeat steps 8 and 9 till you have added all of the words you require to the dictionary.
- 11 Click **Submit** to save the dictionary.

IMPORTING DICTIONARIES

Rather than creating a new dictionary, you can import a ready-made one from elsewhere. There are two ways in which you can import dictionaries into RiskFilter:

- Import a SurfControl dictionary pack
- Import a unicode text file

Importing a SurfControl Dictionary Pack

SurfControl RiskFilter E-mail provides language dictionaries for the following languages:

- Dutch
- French
- German
- Italian
- Japanese
- Portuguese
- Spanish
- Traditional Chinese
- Simplified Chinese

By default, the appliance installs the English language dictionaries but you can add other language dictionaries using the Import-Export utility. Use the Import Dictionaries screen to import dictionaries.

Import Dictionaries	mport Dictionaries				
Dictionaries can be imported from either a Unicode text file or a Surfcontrol dictionary pack xml file. A Unicode text file only contains one dictionary and dictionary information should be specified when importing from a Unicode text file. There should always be a tab space between words and their values in the text file. and there is an option to override if a dictionary with the same name already exists. All dictionaries imported from Unicode text files will be designated as Custom dictionaries. A Surfcontrol dictionary pack/ml) file can contain several dictionaries. When importing from a Surfcontrol dictionary pack file, every dictionary in the pack will be imported. By default, only those dictionary words which have not been changed by users will be imported. There is an option to overwrite any custom changes.					
Select a file and mode					
Select file	Browse				
Select Mode	Import from a Unicode text file				
Import from a Unicode text file	Import from a Unicode text file				
Dictionary Name					
Comment					
Open Message	Display this message when dictionary launches				
Language	English				
Overwrite if the dictionary by the given name already exists					
	Import				

Figure 3 - 12 The Import Dictionaries screen

To import a dictionary:

- 1 Download the SurfControl dictionary pack onto your system from www.surfcontrol.com
- 2 Select Dictionary Manager > Custom Dictionaries from the Policy Manager tab.
- 3 Click Import.
- 4 Enter the path to the dictionary file you downloaded earlier, or click **Browse** and navigate to the location of this dictionary file.
- 5 Select Import from a SurfControl dictionary pack.xml file.
- 6 Select **Overwrite if dictionary by the given name already exists**. If you do not select this option and the dictionary is already in existence, an error will be shown.
- 7 Click Import. You will now see the dictionary in the **Custom Dictionaries** screen.

Creating a unicode text file

Importing a unicode text file is an easy way to add large numbers of words and their scores to a dictionary.

To create a unicode text file:

1 Create a .txt file that has one word and one value per line. Enter the words and dictionary scores you want to add to the dictionary. Put the words in inverted commas (") and put a tab space in between each word and its score. For example:

```
"worthless"(tab space)15
"balance"(tab space)10
```

2 Save the file with a unicode format in a place that can accessed by the RiskFilter appliance.

Importing a unicode text file

To import a text file:

- 1 Select **Dictionary Manager > Custom Dictionaries** from the **Policy Manager** tab.
- 2 Click Import.
- 3 Enter the path to the dictionary file you want to import into the **Select file** field. Alternatively, click **Browse** and navigate to the location of the dictionary file.
- 4 Select Import from a Unicode text file.
- 5 Enter a name for the dictionary into the **Dictionary Name** field.
- 6 Enter text to summarize the dictionary into the **Comment** field if necessary.
- 7 If you want a message to appear when the dictionary is opened enter this message into the **Open Message** pane and select **Display this message when dictionary launches**.
- 8 Choose a language for the dictionary.
- 9 Select **Overwrite if dictionary by the given name already exists**. If you do not select this option and the dictionary is already in existence, an error will be shown.
- 10 Click Import. You will now see the dictionary in the Custom Dictionaries screen.

Exporting a dictionary

You use Dictionary Management to export dictionaries from RiskFilter. This is useful if you want to edit the dictionaries when you are running multiple instances of RiskFilter, because you only have to edit the dictionary once. There are two ways in which you can export Dictionaries:

- As a SurfControl Dictionary pack (an XML file)
- As a unicode file

To export a dictionary:

- 1 Select Dictionary Manager > Custom Dictionaries from the Policy Manager tab.
- 2 You will see a list of all your custom dictionaries. Select the check box alongside the dictionary that you want to export.
- 3 Click **Export**.
- 4 You will see all dictionaries with your chosen dictionary selected. Select any other dictionaries that you want to export.
- 5 Select Export to a Unicode text file or Export to a SurfControl dictionary pack.xml file.
- 6 Click **Export**.



GLOBAL POLICY

RiskFilter provides a global filtering Policy Manager. With this you can define filters, and the actions to be taken when these filters are triggered. Policy and filter configuration is carried out in the Policy Manager tab.



Figure 3 - 13 The Policy Manager tab

The Global Policy Filters screen is where you create and configure the filters that will be used with the global policy and any subsequent policies you create. It enables you to add new filters or edit the filters supplied with the product.

CREATING A NEW SUB-POLICY

Creation and configuration of sub-policies begins in the Global Policy screen. This screen enables you create new policies as well as showing any sub-policies that you already have created.

Globa	Global Policy						
All mes also ov	All messages passing through SurfControl RiskFilter - E-mail will be checked against the Global Policy filters. By default, sub-policies inherit filters from their parent policies. Sub-policies can also overwrite their parent filters to meet their own specific needs.						
lı	ıdex	Order	Sub-policy Name	Edit	Enable		
	1		<u>M</u>	📥 Edit	enable		
					Add Delete		



The policy module of RiskFilter supports infinite policy recursion, i.e., the global policy can include multilevel sub-policies. You can define the corresponding sub-policies according to the different mail routing paths. By default, each level of a sub-policy will inherit the filters enabled by its parent policy (previous level policy). You can modify a sub-policy filter so that it can overwrite the filter defined by its parent policy.



To create a sub-policy:

- 1 Select Global Policy from the Policy Manager tab.
- 2 Click Add. The Sub-policy Management screen is displayed.

Sub-policy Management		
Sub-policy Name		
Sub-policy Status	Enable Disable	
Sub-policy Description	×	

Figure 3 - 15 Enter the details of the new Sub-policy

- 3 Enter a name for your Sub-policy into the **Sub-policy Name** field.
- 4 Select **Enable** in the Sub-policy Status section.
- 5 Enter a brief Sub-policy description.
- 6 Click **Next**. The NewFilter Route screen is displayed.

NewFilter Route					
ID	From	То	Address		
1			Select		
Add Route	Delete Route				
			Submit Ba		

Figure 3 - 16 Enter the relevant route paths

7 Enter the relevant route paths into the **From** and **To** fields. You can directly enter the path, or click **Select** to see a list of all the Address Lists that you have defined.

dress L	.ist	
e following b-policy will	list shows A I be applied.	ddress Groups that you have defined. Select the origin (From) and destination (To) of the messages to which this
rom	To	Address Group
0	0	High (Disable ASA)
0	0	High (Disable AVA)
0	0	Medium (Alert Only)
0	0	Any Address

Figure 3 - 17 Defined Address Groups

- 8 RiskFilter defines the message's route path (Policy Route) by specifying sender and recipient addresses, such as:
 - Specify single sender address to single recipient address: simon@SurfControl.com to tom@SurfControl.com



- Specify single sender address to all users of SurfControl.com domain: simon@SurfControl.com to *@SurfControl.com
- Specify single sender address to all recipients: simon@SurfControl.com to * (* indicates any e-mail address).
- 9 Select which list/s you want to be applied to the filter and click **Submit**.
- 10 If you want to add another route click **Add Route**. To delete a route select the check box to the left of the route and click **Delete Route**.
- 11 Click **Submit** to add this route to your sub-policy. You will now see your new sub-policy within the Global Policy screen.

EDITING A SUB-POLICY

Once you have created a policy, you can edit it at any time.

To edit a policy:

- 1 Select Global Policy from the Policy Manager tab.
- 2 Click Edit. The Sub-policy Management screen is displayed.
- 3 Make the required changes to the policy.
- 4 Click **Submit** to save these new settings.

DELETING A SUB-POLICY

Policies can be deleted when they are no longer needed.

To delete a policy:

- 1 Select **Global Policy** from the Policy Manager tab.
- 2 Select the check box for the policy that you want to delete.
- 3 Click Delete.
- 4 Click **Submit** to save these new settings.

ADDING FILTERS TO THE POLICY

Filters enable you to ask RiskFilter to look for different attributes in messages, then apply an action to them if they match the criteria set up in the filter. The supplied filters consist of:

- Anti-Virus Filter McAfee Enables RiskFilter to stop messages carrying viruses, without any configuration on your part.
- Anti-Spam Filters Heuristics and LexiRules Enable RiskFilter to control spam messages without having to configure anything initially. You can add multiple Anti-Spam filters if necessary.
- Internet Threat Database Filter Compares URL's from SurfControl's Internet Thread Database to the the URL's found in E-mail messages.
- General Content Filter Enables you to do keyword scanning, in the message subject, message body
 or message size.
- Advanced Content Filter Enables you to filter content in the message header, body and attachments more intelligently, with complex keyword expressions.

- Message Attachment Filter Enables you to scan for maximum message size or specify the types of attachments that you want to filter. These include types of attachment, such as *.gif, *.mp3 files, and executable files, such as *.exe and *.dll files by file extension or MIME type.
- Content Guardian Provides maximum flexibility in filtering using SurfControl Content Dictionaries, with multiple filtering arguments.
- Standard Disclaimer filter Adds text to all e-mail messages coming into or out of your organization enabling you to add your own corporate disclaimer easily.



Note: For Global Filtering Policy, all messages will pass through each filter one by one in the global filtering policy until a filter is triggered. When a message triggers a filter (except for the standard disclaimer), the action of this filter will be executed immediately. This message will not pass through all the remaining filters.

When you add a new sub-policy, all of these filters are made available to the new policy with whatever configuration you have set. You cannot edit filters from within a sub-policy, all editing must be done from within the Global Policy Filters menu. Configuration of Global Policy Filters is carried out in the Global Policy Filters screen.

Index	Order	Name	Origin	Туре	Status	
1	Ŷ	Anti-Spam Agent - DFP	Global Policy	Anti-Spam Agent - DFP	enable / read-only	
2	₿	Anti-Spam Agent - Heuristics	Global Policy	Anti-Spam Agent - Heuristics	enable / read-only	
3	₿	Anti-Spam Agent - LexiRules	Global Policy	Anti-Spam Agent - LexiRules	enable / writable	
] 4	រី 🛊	Internet Threat Database	Global Policy	Internet Threat Database Filter	disable / writable	
5	ភិ មិ	HTML Crash?	Global Policy	Advanced Content Filter	enable / writable	
] 6	រីរូ 🛊	Standard Disclaimer	Global Policy	Standard Disclaimer	enable / read-only	
7	貸	Kill test	Global Policy	Content Guardian	enable / writable	

Figure 3 - 18 The Global Policy Filter List screen

DEFINING A FILTER

To add a new filter to your policy, first specify the type of filter that you want to add. This is done in the Create New Filter screen.

ireate New Filter
urfControl RiskFilter - E-mail provides eleven pre-configured filter types. Use this screen to select a new filter to add. Each of these filters enables you to fine-tune your corporate e-mail policy protect against threats such as SPAM, Viruses and Phishing. Note: Some filters are not available for adding more than once, so they might not be listed here.
Select a filter type
O Internet Threat Database Filter
⊙ General Content Filter
O Advanced Content Filter
O Message Attachment Filter
O Content Guardian
O Dictionary Threshold Filter
Next Cancel

Figure 3 - 19 Supplied Filters



Creating a new filter

To create a new filter:

- 1 In the Global Policy Filter List screen click Add. The Create New Filter screen is displayed.
- 2 Select the type of filter that you want to create. Details of the different types of filter available are covered in the following sections.
- 3 Click Next.
- 4 Fill in the properties for the filter that you want to create and click **Submit**.

Once you have added one of the following filters you will be unable to add another filter of the same type. You will not be able to select them in the Create New Filter screen though you will be able to edit them by clicking the corresponding link in the Global Policy Filter List screen. The filters are:

- Anti-Virus Agent McAfee
- Anti-Spam Agent DFP
- Anti-Spam Agent Heuristics
- Anti-Spam Agent LexiRules
- Standard Disclaimer

THE ANTI-VIRUS AGENT FILTER

The Anti-Virus Agent filter is supplied with the product and enabled by default. This means that it will filter messages automatically without any prior modification. The McAfee filter provides fast, reliable inline virus filtering and is a RiskFilter standard.

Editing the Anti-Virus Agent Filter

You can fine-tune the Anti-Virus Agent filter to your company's filtering requirements.

To edit the Anti-Virus Agent Filter:

- 1 Select Global Policy > Filters from the Policy Manager tab.
- 2 Click Add. The Create New Filter screen is displayed.
- 3 Select the Anti-Virus Agent that you want to edit and click **Next**.
- 4 If you want to change the name of this filter, enter a new name into the **Filter Name** field.
- 5 Select disable if you want to switch the filter off.
- 6 Change the Filter Permission setting to writable to enable the filter to be overwritten by a sub-policy.



Note: If the Anti-Virus Agent (AVA) filter is enabled in a global policy, it cannot be enabled in, then overwritten by, a sub-pulicy. For example: You can enable McAfee in one global policy, and then enable it in a sub policy that is attached to a different global policy. You cannot, however, enable it in a global policy and its sub-policy at the same time.

- 7 Configure how you want the filter to scan messages for viruses:
 - **Treat errors as infected** If any errors are encountered during the scanning of a message, the file will be assumed to be infected. The default setting is **on**.

- Treat encrypted files as infected If a message is encrypted in a way that the anti-virus engine does not understand, it will be assumed to be infected and treated as such. The default setting is on.
- **Treat macros as infected** If a file contains macros, it will be treated as an infected file. This is **off** by default and is only available with the McAfee filter.
- Heuristics Analysis Used if an unknown virus is found. This is on by default.
- Macro Analysis Used if an unknown macro virus is found. This is on by default.
- Scan all files for viruses Scans all files, regardless of file extension. This is off by default.
- **Malicious applications** Scans for potentially harmful applications such as password crackers. Also scans for some joke programs. This is **on** by default.
- Joke/Hoax Viruses Scans for Hoax/Joke programs. This is on by default.
- Scan message body for viruses Scans the message body for embedded malicious scripts or attachments that can't be scanned properly. If, because of message format problems, attachments are seen as part of the message body, they will still be scanned and viruses picked up.
- 8 Configure how you want messages to be treated if they contain a virus:
 - **Clean virus –** Select this option if you want RiskFilter to try to clean a virus if it finds one. This is a good option if you are not sure that you want attachments deleted without checking, but at the same time don't want them stored on the appliance. You can also select the check box beneath this option to ask for the attachment to be deleted if the virus cannot be cleaned.
 - Remove the infected attachment files Deletes the attachment and virus automatically.
 - Keep (no action taken) This is the default action. The attachment and virus is stored in a predefined location and, if required, a message is sent to the administrator stating that a virus has been found. This message can be edited if necessary.
 - Insert a notice when a message is delivered with a virus Enables you to configure a message to be sent to the administrator when a virus is found. You can choose where the notice is positioned within the message.
- 9 Set the action that will be taken if the filter is triggered. See "Step 2 Defining the action" on page 67 for details on what these actions are.
- 10 Click **Submit** to save these new settings.



THE ANTI-SPAM AGENT FILTERS

The Anti-Spam filters check messages to see if they are likely to be spam.

- Anti-Spam Agent DFP Compares mail messages to known spam from different categories.
- Anti-Spam Agent Heuristics Uses regular expressions to determine the likelihood that an e-mail message is actually Spam.
- Anti-Spam Agent LexiRules Analyses words, phrases and patterns commonly found in spam to identify e-mail messages as possible spam.

You can fine-tune the Anti-Spam Agent filters to your company's filtering requirements. All of the filters can be edited in their corresponding property screen.

Configuring the Digital Fingerprinting (DFP) Anti-Spam Agent Filter

The Digital Fingerprinting Anti-Spam Agent filter is configured in the Anti-Spam Agent DFP screen.

Anti-Spam Agent - DFP			
The Digital Fingerprinting (DFP) Filter	compares mail messages to known spam in different categories.		
Filter Property			
Filter Name	Anti-Spam Agent - DFP		
Filter Status	⊙ enable ○ disable		
Filter Permission	O writable ⊙ read-only		
Filter Criteria			
Adult Adult			
Chain Letters			
Computing & Internet			
Dating & Personals			
Entertainment			
Finance & Home Business			
Gambling			
Games & Interactive			
Health & Medicine			
Humor			
🕑 Illegal Material			
Novelty Software			
✓ Offensive			
Phishing & Fraud			
Products & Services			
Special Events			
Other			
Check All Uncheck All			
	Bypass Anti-Spam Agent scanning if message size is more than 10 KB		
Action if filter triggered			
Modify Subject			
X-Header			
Copy To			
Save to	junkmail 🗸		
Send Notification			
O Deliver Message			
Dron Massana			

Figure 3 - 20 The Anti-Spam Agent - DFP screen

To configure the DFP Anti-Spam Agent filter:

- 1 Select **Global Policy** from the **Policy Manager** tab.
- 2 Click Filters. The Global Policy Filter list screen is displayed.
- 3 Click Add. The Create New Filter screen is displayed.
- 4 Select Anti-Spam Agent DFP.

Note: You will only see this if you have not added an Anti-Spam Agent -DFP filter previously

5 Click Next.



Configuring the Anti-Spam Agent - Heuristics Filter

The Anti-Spam Agent - Heuristics filter is configured in the Anti-Spam Agent Heuristics screen.

Anti-Spam Agent - H	Heuristics
The Heuristics Rules Filter	r uses regular expressions to determine the likelihood that an e-mail message is actually spam.
Filter Property	
Filter Name	Anti-Spam Agent - Heuristics
Filter Status	⊙ enable ⊘ disable
Filter Permission	O writable ⊙ read-only
Filter Criteria	
Filter Co	O Lowest - detects the least spam but decreases the risk offalse positives. O Low - detects less spam but decreases the risk offalse positives. O Medium - medium spam detection and false positives. O High - detects more spam but increases the risk offalse positives. O High - detects more spam but increases the risk offalse positives. O Highest - detects more spam but increases the risk offalse positives.
	Scan message headers only
	☑ Bypass Anti-Spam Agent scanning if message size is more than 50 KB
Action if filter triggere	ed
🔲 Modify Subject	
X-Header	
🗌 Сору То	
Save to	junkmail 🔽
Send Notification	
O Deliver Message	
 Drop Message 	
	Submit

Figure 3 - 21 The Anti-Spam - Heuristics screen

To cofigure the Anti-Spam Agent - Heuristics filter:

- 1 Select Global Policy from the Policy Manager tab.
- 2 Click Filters. The Global Policy Filter list screen is displayed.
- 3 Click Add. The Create New Filter screen is displayed.
- 4 Select Anti-Spam Agent Heuristics.

Note: You will only see this if you have not added an Anti-Spam Heuristics Filter previously.

5 Click Next.

- 6 Enter a name into the Filter Name field.
- 7 This filter is enabled by default. Select the 'disable' option if you want to switch it off.
- 8 If you want to make the filter so that it can be overwritten by a sub-policy change the **Filter Permission** setting to **writable**. The default is **read-only**.
- 9 Select the Sensitivity Level. This sets how strictly RiskFilter scans messages:
 - **Lowest** You should not get any false positives with this setting but it is very likely that some spam messages will not be stopped.
 - Low Only messages that are definitely spam will be stopped. With this setting, false positives will be less but you also run the risk of messages that are spam getting through.
 - Medium More messages will be stopped as the criteria for deciding whether a message is spam or not, is much wider. However, some messages that are not spam may be stopped.



- **High** Any message that could be spam will be stopped. Although this offers the most comprehensive protection, more messages will be stopped that are not spam.
- Highest Virtually all spam will be stopped but there could be quite a few false positives. With this
 setting it is advisable to check all spam before deleting, just in case.
- 10 Select **Scan only message headers** if you want RiskFilter to only scan the header, not the body of the message.
- 11 Select **Bypass Anti-Spam Agent scanning if message size is more than ... KB** and set a maximum message size. This means that any message that is particularly large will not be scanned as possible spam. The default setting is 100KB.
- 12 Set the action that will be taken if the filter is triggered. See **Step 2 Defining the action on page 67** for details on what these actions are.
- 13 Click **Submit** to save these new settings.

Configuring the Anti-Spam Agent - LexiRules Filter

The Anti-Spam Agent - LexiRules filter is configured in the Anti-Spam Agent LexiRules screen.

Anti-Spam Agent	Anti-Spam Agent - LexiRules				
The LeviRules Filter analyses words, phrases and patterns commonly found in sparn to identify e-mail messages as possible sparn.					
Filter Property					
Filter Name		Anti-Spam Agent - LexiRules			
Filter Status		⊙enable O disable			
Filter Permission		⊙viritable O read-only			
Filter Criteria					
	Filter Component	s Anti-Spann Agent - LexiRules			
		J Bypass Anti-Spam Agent scanning it message size is more than 10 KB			
Action if filter trigge	ered	Instant -			
Modify Subject		test to st			
X-Header					
Сору То		fds@asdf.com			
Save to		Junkmail 💌			
Send Notification					
	Sender	O Original E-Mail Sender			
		O Administrator			
		OUserSpecified			
		statford home@shoms.surfcontrol.com			
	10	Original E-Mail Sender			
		L) Orginal E-Mail Receiver(s)			
		Liuserspectned			
		Separate each entry with a semicolon()			
	Subject	WARNING: Inappropriate e-mail message			
	Message Content	The message sent to %RCPT8% on %DATE&TIME%			
		Sender: %SENDER% Message subject: %SUBJECT%			
		O Do not attach message			
		CAttach modified message			
0.00		C Austri organiarinessage			
Deriver message					
C Diole wessage		[Submit] [Reset]			

Figure 3 - 22 The Anti-Spam Agent - LexiRules filter

To configure the Anti-Spam Agent - LexiRules filter:

- 1 Select Global Policy from the Policy Manager tab.
- 2 Click Filters. The Global Policy Filter list screen is displayed.
- 3 Click Add. The Create New Filter screen is displayed.
- 4 Select Anti-Spam Agent LexiRules.

Note: You will only see this if you have not added an Anti-Spam LexiRules Filter previously



- 5 Click Next.
- 6 Enter a name in to the **Filter Name** field.
- 7 This filter is enabled by default. Select the **disable** option if you want to switch it off.
- 8 If you want to make the filter so that it can be overwritten by a sub-policy change the **Filter Permission** setting to **writable**. The default is **read-only**.
- 9 Select Bypass Anti-Spam Agent scanning if message size is more than ... KB and set a maximum message size. This means that any message that is particularly large will not be scanned as possible spam. The default setting is 100KB.

INTERNET THREAT DATABASE FILTER

The Internet Threat Database Filter enables you to maximise message filtering by using SurfControl's database of 9 Million URLs. Each category contains a list of URLs that have been added and are constantly updated by a team of SurfControl researchers. These categories enable you to apply a rule to a group of URLs rather than having to enter each one individually.

You also have the option to add specific URLs that are not covered in the categories already provided. Configuration of the Internet Threat Database Filter is carried out in the Internet Threat Database Filter screen.

Internet Threat Database Filter				
The Internet Threat Database Fi categories of URLs to scan for.	ter compares URLs from SuffControl's Internet Thread Database to the URLs found in e-mail messages. This filter can be refined by selecting specific			
Filter Property				
Filter Name	Internet Threat Database			
Filter Status	⊖ enable ⊙ disable			
Filter Permission	⊙ writable O read-only			
Filter Criteria				
Adult/Sexually Explicit				
🗹 Criminal Skills				
🗹 Drugs, Alcohol & Tobacco				
🗹 Gambling				
Hacking				
Hate Speech				
Violence				
Veapons 🗸				
Check All Uncheck All				
	Bypass Anti-Spam Agent scanning if message size is more than 10 KB			
Action if filter triggered				
🔲 Modify Subject				
X-Header				
🗌 Сору То				
Save to	junkmail 💌			
Send Notification				
O Deliver Message				
Drop Message				
	Submit)Reset			

Figure 3 - 23 The Internet Threat Database Filter screen



Editing the Internet Threat Database Filter

You can fine-tune either (or both) of the Internet Threat Database filter to your company's filtering requirements.

To edit the Internet Threat Database filter:

- 1 Select Global Policy from the Policy Manager tab.
- 2 Click Filters. The Global Policy Filter list screen is displayed.
- 3 Click Add. The Create New Filter screen is displayed.
- 4 Select the Internet Threat Database Filter and click Next.
- 5 Enter a new name into the **Filter Name** field to change the name of this filter.
- 6 This filter is enabled by default. Select **disable** if you want to switch it off.
- 7 If you want to make the filter so that it can be overwritten by a sub-policy change the **Filter Permission** setting to **writable**. The default is **read-only**.
- 8 Select the categories that you want to apply the filter to (for descriptions of these categories see Internet Threat Database Categories on page 165):
 - Adult/Sexually Explicit
 - Criminal Skills
 - Drugs, Alcohol & Tobacco
 - Gambling Hacking
 - · Hate Speech
 - Violence
 - Weapons
- 9 Click **Submit** to save these new settings.

STANDARD DISCLAIMER

Standard Disclaimer enables you to add corporate disclaimers to the top or bottom of the message body. When the recipient receives the message, they will see the disclaimer in their message. You can configure different disclaimers by adding the standard disclaimer to the sub-policy.

Standard Disclaimer					
- Standard Disclaimer enables you to append text to specified messages. You can append the text at the beginning or at the end of the message.					
Filter Property	Filter Property				
Filter Name	Standard Disclaimer				
Filter Status	⊙ enable ○ disable				
Filter Permission	O writable ⊙ read-only				
Standard Disclaimer content					
	This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed.				
Position of Standard Disclaimer					
	O At the beginning of the message body				
	⊙ At the end of the message body				
	Submit)Reset				

Figure 3 - 24 The Standard Disclaimer screen



For example, if you have added two sub-policies, Incoming and Outgoing, you could create disclaimers for each of them:

- · Global Policy 'Innovation makes your life better'
- · Incoming 'All messages have been scanned by RiskFilter'
- Outgoing "Powered by RiskFilter"

We recommend that you put the Standard Disclaimer filter at the end of the filter list in the Global Policy Filter List screen and that you do not include words in the message that are keywords for other filters. This will make sure that any messages carrying the Standard Disclaimer are not stopped by other filters (such as Anti-Spam) once it has been added. It also makes sure that the Standard Disclaimer is not unnecessarily added to messages that are then stopped for other reasons.

Editing the Standard Disclaimer Filter

You can edit this filter to exactly match your company's requirements.

To edit the Standard Disclaimer filter:

- 1 Select Global Policy from the Policy Manager tab.
- 2 Click Filters. The Global Policy Filter list screen is displayed.
- 3 Click Add. The Create New Filter screen is displayed.
- 4 Select the Standard Disclaimer Filter.



- 5 Click Next.
- 6 Enter a new name into the Filter Name field to change the name of this filter.
- 7 This filter is enabled by default. Select the disable option if you want to switch it off.
- 8 If you want to make the filter so that it can be overwritten by a sub-policy change the **Filter Permission** setting to **writable**. The default is **read-only**.
- 9 Enter the text that you want RiskFilter to add to e-mail messages by entering your own message into the Standard Disclaimer Content screen.



- 10 Specify where you want your disclaimer to be put within the message:
 - At the beginning of the message body The disclaimer will placed at the top of the message.
 - At the end of the message body The disclaimer will placed at the end of the message.
- 11 Click **Submit** to save these new settings.



GENERAL CONTENT FILTER

The General Content Filter enables you to filter all incoming and outgoing messages passing through the RiskFilter.

General Content Filter	
SurfControl RiskFilter - E-mail Gen subject line and/or message body.	aral Content Filter enables you to screen your e-mail for specific content. The General Content Filter can perform keyword searches in the message It can also filter based on message size.
Filter Property	
Filter Name	
Filter Status	⊙ enable O disable
Filter Permission	⊙ writable O read-only
Filter Criteria	
Subject line Separate multiple subject line	s with a semicolon (,)
Match case	
Mail body contains All keywor Separate each keyword with a	ds 🗸
📃 Match case	
Message size is greater than	KB KB
Action if filter triggered	
Modify Subject	
X-Header	
📃 Сору То	
Save to	quarantine 🗸
Send Notification	
O Deliver Message	
⊙ Drop Message	
	Submit

Figure 3 - 25 General Content Filter screen

Editing the General Content Filter

You can edit this filter to exactly match your company's requirements.

To edit the General Content filter:

- 1 Select Global Policy from the Policy Manager tab.
- 2 Click Filters. The Global Policy Filter list screen is displayed.
- 3 Click Add . The Create New Filter screen is displayed.
- 4 Select the General Content Filter and click Next.
- 5 Enter a new name into the **Filter Name** field to change the name of this filter.
- 6 This filter is enabled by default. Select **disable** if you want to switch it off.
- 7 If you want to make the filter so that it can be overwritten by a sub-policy change the **Filter Permission** setting to **writable**. The default is **read-only**.



ADVANCED CONTENT FILTER

The Advanced Content Filter provides more complex checking of message header, message body and message attachments and supports the dynamic evaluation of keyword frequency to enhance flexibility.

Advanced	d Content Filter			
The SurfCont expressions. filter's sensiti	rol RiskFilter - E-mail A Dictionary support is ir vity to keyword matches	dvanced Content Filter enables you to fil cluded, enabling easy selection of keyw , when deciding whether to trigger the fil	ier content in the message header, message body and message ords from one of the categories. Advanced Content Filter support ter.	attachment for simple and complex s keyword frequency and configuration of a
Filter Prop	perty			
Filter Name				
Filter Status		⊙ enable O disable		
Filter Permis	sion	⊙ writable ◯ read-only		
Filter Crite	eria			
Select the filt	ering target to compare der	with the listed expressions.		
📃 Subj	ect 🗌 From 🔲 To 🛛	Cc Other		
📃 Mail bod	У			
📃 Mail atta	Mail attachment			
Scan for	Scan for archives with (up to 15) 3 layers			
📃 Strip	attachment			
Expression	n List			
Index	Enable	Expression	Case Sensitive	Delete Add Delete
	Enable Level of	Severity		
	Severity threshol	d 1		
Action if f	ilter triggered			
📃 Modify S	ubject			
🗌 X-Heade	r			
🗌 Сору То				
Save to		quarantine 🖌		
Send No	tification			
O Deliver N	lessage			
📀 Drop Me	ssage			
				Submit Reset

Figure 3 - 26 The Advanced Content Filter screen

Editing the Advanced Content Filter

You can edit this filter to exactly match your company's requirements.

To edit the Advanced Content filter:

- 1 Select Global Policy from the Policy Manager tab.
- 2 Click Filters. The Global Policy Filter list screen is displayed.
- 3 Click Add. The Create New Filter screen is displayed.
- 4 Select the Advanced Content Filter and click Next.

Using the Expression List

A valid keyword expression is composed of keywords and logical operators. You can enter keyword expressions by either typing them manually or choosing them from the Content dictionaries. The Content dictionaries also have about 20 categories with approximately 14,600 keywords. If you are going to be using keyword checks then you need to add them to the Expression List section.

To configure Expression lists:

1 Click Add. The Expression screen is displayed.

Expression		
There are three types of operators currently supported by the SurfControl RiskFilter: AND, OR and OCCUR. Only one type of the operators is allowed in an expression, but it can be used multiple times in the same expression. To select words from one of the SurfControl Content Dictionaries, click on the Dictionary icon below.		
Enable	 ● Enable ○ Disable 	
Expression	Select SurfControl Content Dictionary) e.g., keyword1 <and> keyword2 keyword1 <or> keyword2 <occur> keyword</occur></or></and>	
Case Sensitive	 ○ Yes ("ABC" ⊨ "abc") ● No ("ABC" = "abc") 	
Frequency	1 times (Only applies to <occur> operator)</occur>	
	Submit Cancel	

Figure 3 - 27 The Expression screen

- 2 Select **Enable** to activate the Expression.
- 3 Enter an expression into the field by manually entering it (see Using Logical Operators on page 94' for details on how to do this). Alternatively, click Select SurfControl Content Dictionary. The Content Dictionaries dialog box is displayed.

🗿 SurfControl RiskFilter - E-mail - Microsoft Internet Expl 📃 🗖 🔀			
Dictionaries			
Select words fr selected by us	om the dictionarie ing the CTRL key.	s listed belov	v. Multiple words can be
Language	All	~	
Dictionary	Adult * Dictionaries		× Surfcontrol
Words	freepic jerk off liplocked cleavage zoophilia ass flasher doggie style	<	
Operator	O <and> multiple selections ⊙ <or> multiple selections</or></and>		
			Select Close 🤍

- 4 Select the following:
 - **Language** the Content dictionaries have eight languages: English, Simplified Chinese, Traditional Chinese, German, French, Italian, Spanish and Japanese.



Note: By default, the Content Dictionaries dialog opens with the 'Adult' dictionary in view. This shows a list of words that are offensive.



- 5 **Dictionary Category** the type of dictionary that you need to use is defined by the style of message you want to filter.
- 6 Select the logical operator that you want to use in this expression (see Using Logical Operators on page 94 for more details):
 - <AND> multiple selections This filter will trigger if one of the selected keywords AND another selected keyword appear in the message. If only one of these words appears in the message the filter will not trigger.
 - <OR> multiple selections This filter will trigger if either one of the selected keywords appears in the message.

You can also add an **<OCCUR>** to the filter to specify how many times the keyword/s must appear before the filter is triggered.

1 Click **Select**. Once you have entered your expression either by adding it manually or by clicking **Select** from the Content Dictionaries it will appear in the Expression List section.



Note: You can add multiple expressions to complete the filtering content.

- 2 Specify whether you want the case of the words to be considered by selecting 'Yes' or 'No' in the Case Sensitive section.
- 3 If you have added an **<OCCUR>** operator to your expression to specify how often the word must appear in the message, you can check the **Enable Level of Severity** option. RiskFilter will compare the frequency of the expression triggering in the mail header, mail body and mail attachment with the threshold value entered in the **Severity Threshold** field. If the frequency is greater than this value, RiskFilter will perform the pre-configured filter actions.
- 4 Click **Submit** to save these new settings.

Using Logical Operators

The Advanced content filter now supports three types of logical operator: **<OR>**, **<AND>** and **<OCCUR>**.

- <OR> An expression with an <OR> operator checks whether either of the keywords, 'one before' and 'one after' the operator, appears. If either keyword does appear, the expression is a match.
- <AND> An expression with an <AND> operator checks whether both of the keywords appear. If they
 do, the expression is a match. If just one keyword appears, the expression is not a match.
- <OCCUR> An expression with an <OCCUR> operator checks the frequency of the keywords in the
 expression. If the number of occurrences of the keyword in the expression is equal to or greater than
 the value set by Frequency, this expression will be a match. The default value for Frequency is 1.



Examples showing the use of Operands

The following examples show how operands can be inserted and how RiskFilter will use them to decide whether to trigger the action defined in the Advanced Content Filter:

RiskFilter <AND> Gateway <AND> Innovation

This expression matches content when "RiskFilter", "Gateway" and "Innovation" are all present.

nesuit
Matches
Does not match
Does not match

RiskFilter <OR> Gateway <OR> Innovation

This expression matches content when "RiskFilter", "Gateway" or "Innovation" is present.

Content	Result
Welcome to SurfControl RiskFilter for a secure mail gateway solution!	Matches
Welcome to SurfControl RiskFilter home page!	Matches
For a secure e-mail server solution, you are welcome to contact us.	Does not match

<OCCUR> gateway

(Assume Frequency =2)

This expression matches content if "gateway" occurs more than twice.

Content	Result
Welcome to SurfControl Risk Filter - E-mail for a secure mail gateway solution!	Does not match
Innovation gateway provides a securegateway	Does not match
For a secure mail gateway solution, checkgatewayand Innovation gateway is high performance	Matches

Multiple operators can be used in a single keyword expression, but multiple operator types are not allowed in a single dynamic keyword expression.

For example: RiskFilter<OR>Gateway<AND>Innovation is an invalid keyword expression.

Valid keyword expression examples:

- RiskFilter
- innovation
- RiskFilter <AND> innovation



- RiskFilter <AND> innovation <AND> Solution
- RiskFilter <OR> innovation
- RiskFilter <OR> innovation <OR> Messaging Gateway
- <OCCUR> RiskFilter
- <OCCUR> RiskFilter <OCCUR> Innovation



Caution: Do not use operands in isolation, for example: <AND>. They must always accompany a word: for example, RiskFilter <AND>, or RiskFilter <AND> SurfControl. An error will be shown if an operand is entered without an accompanying word.

MESSAGE ATTACHMENT FILTER

The Message Attachment filter allows you to choose or add the types of attachment that you want to filter, including MIME sub-types, such as *.gif, *.mpeg files, and executable files, such as *.exe and *.dll files.

Naccara Attachmant Eilter			
Message Allaci ille il Fille i			
The SurfControl RiskFilter - E-ma	il Message Attachment Filter enables you to specify message attachment attributes to scan for.		
Eilter Preperty			
Filter Name			
Filter Status	⊙ enable ⊙ disable		
Filter Permission	⊙ writable O read-only		
Attachment			
	Scan for file names using patterns. Use a semicolon () to separate multiple patterns. Note: spaces are included as part of the search pattern		
	Scan for selected attachment file types.(Edit.)		
	Scan for archives with (up to 15) 3 layers		
	Scan for archives which have a decompressed size greater than (up to 1000 MB) 20480 KB		
	Strip and discard the attachment when a scanning criteria is met		
Action if filter triggered			
Modify Subject			
X-Header			
Сору То			
Save to	quarantine 🗸		
Send Notification			
O Deliver Message			
 Drop Message 			
	Submit)Reset		

Figure 3 - 28 Message Attachment Filter screen



3

Editing the Message Attachment Filter

You can edit this filter to exactly match your company's requirements.

To edit the Message Attachment filter:

- 1 Select Global Policy from the Policy Manager tab.
- 2 Click Filters. The Global Policy Filter list screen is displayed.
- 3 Click the Add .The Create New Filter screen is displayed.
- 4 Select the Message Attachment Filter and click Next.
- 5 Enter a new name into the field to change the name of this filter.
- 6 This filter is enabled by default. Select the **disable** option if you want to switch it off.
- 7 If you want to make the filter so that it can be overwritten by a sub-policy change the **Filter Permission** setting to **writable**. The default is **read-only**.
- 8 Specify how you want RiskFilter to deal with attachments:
 - Scan for file names using patterns. Use a semicolon (;) to separate multiple patterns Searches for patterns in file names i.e. image.jpg, a*t, About.
 - Scan for selected attachment file types (Edit) Will scan for the selected file types including those within archives. Click Edit. A screen is displayed where you can define exactly what type of file you want to scan.
 - Scan for archives (up to 15) ... layers The e-mail attachment will be scanned to see if it has more layers than the number defined in the Filter Criteria section. If it does have more layers, it will be treated in the way specified for that filter if it is triggered.
 - Scan for archives which have a decompressed size greater than (up to 1000MB) ... KB E-mail messages with archives are checked to ensure the unzipped size does not exceed this value.
 - Strip and discard the attachment when filtering criteria met If this option is selected and the filter is triggered the attachment will be removed from the message and discarded.
- 9 Set the action that will be taken if the filter is triggered. See **Step 2 Defining the action on page 67** for details on what these actions are.
- 10 Click **Submit** to save these new settings.



CONTENT GUARDIAN

RiskFilter Content Guardian provides a more intelligent and flexible filtering method. The filtering criteria of Content Guardian consists of one or more filtering rule(s) which are made up of three parts: filtering target, matching condition, and filtering content. When matching conditions are met, the filter will trigger.

Content Guardian		
SurfControl RiskFilter - E-mail C allowing the easy selection of k Content Guardian rule.	tent Guardian provides maximum flexibility by filtering all components of an e-mail message. Content Guardian also gives you access to Dictionaries, ords from specific content categories. In addition, you can set the criteria for how many filtering arguments must be met, before an e-mail triggers the	
Filter Property		
Filter Name		
Filter Status	⊙ enable O disable	
Filter Permission	⊙ writable O read-only	
Filter Criteria		
The condition for the following r	s is All of the items match 🔹 💌	
Sender IP address	🔹 is 💌	
Delete Add		
Action if filter triggered		
📃 Modify Subject		
X-Header		
📃 Сору То		
Save to	quarantine 🗸	
Send Notification		
🔘 Deliver Message		
⊙ Drop Message		
	Submit	

Figure 3 - 29 Content Guardian

Creating a new Content Guardian filter

You can edit the supplied filter to exactly match your company's requirements.

To edit the Content Guardian filter:

- 1 Select Global Policy from the Policy Manager tab.
- 2 Click Filters The Global Policy Filter list screen is displayed.
- 3 Click Add. The Create New Filter screen is displayed.
- 4 Select the Internet Content Guardian Filter and click Next.
- 5 Enter a new name into the **Filter Name** field to change the name of this filter.
- 6 This filter is enabled by default. Select the disable option if you want to switch it off.
- 7 If you want to make the filter so that it can be overwritten by a sub-policy change the **Filter Permission** setting to **writable.** The default is **read-only**.
- 8 Select a filtering rule from the **The condition for the following rule is** list:
 - All of the items must match
 - Any of the items match
 - Not all of the items match
 - None of the items match



- 2 of the items match
- 3 of the items match
- 4 of the items match
- 5 of the items match
- 9 Each different filtering target has the appropriate matching condition(s). Choose one of the targets from the drop-down list:
 - Is
 - Is not
 - Contains
 - Does not contain
 - Matches (wildcard character * and ? supported)
 - Does not match (wildcard character * and ? supported)
 - Matches regular expression
 - Does not match regular expression
 - Equals
 - · Does not equal to
 - Is less than
 - Is less than or equal to
 - Is greater than
 - Is greater than or equal to
- 10 Enter a matching value (such as keywords, e-mail address, 1024KB and others) into the field to the right of the matching conditions.
- 11 RiskFilter executes filtering rules in turn, and checks whether the condition matches a rule which can be triggered. If you need to adjust the order of the filtering rules, click the Adjust icon on the left, and adjust as required.
- 12 Set the action that will be taken if the filter is triggered. See **Step 2 Defining the action on page 67** for details on what these actions are.
- 13 Click **Submit** to save these new settings.

Adding a filtering rule

To add a filtering rule you need to can add a new Content Guardian filter.

To add a new Content Guardian filter:

- 1 Select Global Policy from the Policy Manager tab.
- 2 Click Filters. The Global Policy Filter list screen is displayed.
- 3 Click Add. The Create New Filter screen is displayed.
- 4 Select Content Guardian and click Next.
- 5 Click **Add** in the Filter Criteria section.
- 6 New fields will appear beneath the existing rule/s where you can specify conditions for your new rule.



7 Click Submit to save these new settings.

Deleting a filtering rule

You can delete a filtering rule that is no longer needed.

To delete a filtering rule:

- 1 Select Global Policy from the Policy Manager tab.
- 2 Click **Filters**. The Global Policy Filter list screen is displayed.
- 3 Click Add. The Create New Filter screen is displayed.
- 4 Select Content Guardian and click Next.
- 5 Select the check box alongside the rule that you want to delete.
- 6 Click **Submit** to save these new settings.

DICTIONARY THRESHOLD FILTER

The Dictionary Threshold Filter uses a library of dictionaries that contain words associated with different aspects of unwanted content. RiskFilter is pre-configured with the following dictionaries:

Adult, Alcohol/Tobacco/Drugs, Arts/Entertainment, Computing/Internet/hacking, Confidential, Finance, Gambling, Hate speech/Offensive, Job search, Medical/Healthcare, Shopping, Spam, Spam Misspellings, Sports, Travel and Violence/Weapons.

How the Dictionary Threshold Filter works

The Dictionary Threshold filter works by assigning each word a numeric value. It then checks to see how many words from the selected dictionaries appear within a message and adds up the total. If this value is greater than the value specified in the Dictionary Threshold filter, the filter will trigger.

EXAMPLE: a Dictionary Threshold value of 150 from the Gambling dictionary is set for a rule. An e-mail using the words 'baccarat', 'blackjack', 'poker' and 'slot machine', arrives at the SurfControl server. The dictionary value of each of these words is 50, making a total of 200. This exceeds the Dictionary threshold value and the filter triggers.

Dictionary Threshold Filter Dictionary Threshold Filter triggers when a Message's score for the selected Dictionary is equal to or greater than the defined Threshold for the selected Message Parts Filter Property Filter Name 📀 enable Filter Status O disable writable Filter Permission O read-only Filter Criteria Select the filtering target to compare with the listed expression Mail header Subject From To Cc Other Mail body Mail attachment Scan for archives with (up to 15) 3 layers Strip attachment Select Dictionary 111 222 DE_Accounting * DE_Alkohol/Tabak/Drogen * DE Computing/Internet/Hacking * DE Erwachsene * DE_Gewalt/Waffen * DE_Glücksspiele * DE_Kunst/Unterhaltung * DE_Jobsuche *

Dictionary Thresholds are configured in the Dictionary Threshold screen.

Figure 3 - 30 The Dictionary Threshold Filter screen





Configuring the Dictionary Threshold Filter

To configure the Dictionary Threshold Filter you need to specify:

- What kind of content you want the rule to detect.
- · Which parts of the e-mail message you want to scan for dictionary content.
- The dictionary score required to trigger the rule.

You can edit this filter to exactly match your company's requirements.

To edit the filter:

- 1 Select Global Policy from the Policy Manager tab.
- 2 Click Filters. The Global Policy Filter list screen is displayed.
- 3 Click Add . The Create New Filter screen is displayed.
- 4 Select the **Dictionary Threshold Filter** and click **Next**.
- 5 Enter a name for this filter into the **Filter Name** field.
- 6 This filter is enabled by default. Select **disable** if you want to switch it off.
- 7 If you want to make the filter so that it can be overwritten by a sub-policy change the **Filter Permission** setting to **writable**. The default is **read-only**.
- 8 Select the check boxes that correspond to the parts of the message that you want to be checked against the dictionary you have chosen. RiskFilter will then check the specified part/s of the message to see if the specified words appear in it and whether the resulting threshold value is high enough to trigger the filter:
 - **Mail Header** Ask RiskFilter to check the message header for the the dictionary word then specify which part of the header you want it to check.
 - **Subject** the text in the 'Subject' field will be checked.
 - From the text in the 'From' field will be checked.
 - **To** the text in the 'To' field will be checked.
 - **Cc** the text in the 'Cc' field will be checked.
 - Other enter any other attribute that may appear in the header for RiskFilter to look for. For example: enter 'Message -Id' for RiskFilter to scan the message-id of the header.
 - Mail Body Ask RiskFilter to check the message body for the dictionary word.
 - **Mail Attachment –** Ask RiskFilter to check attachments for the dictionary word. You specify how many layers within an attachment should be scanned. This is useful for looking for embedded files such as data sheets within text documents.
- 9 Select the 'Strip attachment' check box to have the attachment removed if the filter is triggered.
- 10 Select the dictionary that you want to be used by the filter. Multiple dictionaries can be selected and **Check All** can be used to select them all.



11 Enter the Dictionary Threshold value for this filter into the **Dictionary Threshold** field.

Select Threshold	
Dictionary Threshold	100
Action if filter triggered	
Modify Subject	
X-Header	
🗖 Сору То	
Save to	quarantine 💌
Send Notification	
O Deliver Message	
 Drop Message 	
	Submit Reset

Figure 3 - 31 Enter the Dictionary Threshold value into the Select Threshold section

- 12 Set the action that will be taken if the filter is triggered. See Step 2 Defining the action on page 67 for details on what these actions are.
- 13 Click **Submit** to save these new settings.



KEY POINTS

The following list is a summary of the main points covered in Chapter 3. Use this list as a quick reminder of what you can do within the Policy Manager tab:

- You can apply different filtering solutions to messages from specific address groups, according to different routing paths.
- There are three ways to add an e-mail address: Add the address/es manually, import the address/es from a file or import the address/es from an LDAP connection.
- Filter action is set when you create a new filter, within that filter's configuration screen.
- Rules are defined by creating filters that set the contraints, and action to be taken, on messages that trigger one of these filters.
- All messages passing through SurfControl RiskFilter E-mail will be checked against the Global Policy filters.
- By default, sub-policies inherit filters from their parent policies. Sub-policies can also overwrite their parent filters to meet their own specific needs.
- You can add one or more address group to the address group list, and each address group can include a group of e-mail address lists.
- If you already have a list of domain or e-mail addresses to apply your policy to, you can import this list into Policy Manager and use it in your policy.
- You can export a list of IP addresses to another appliance.
- You can delete address groups that you no longer require.
- When a message triggers a filter it can be sent to a queue, where it can be stored until you are ready to deal with it.
- The default queues are:
 - Virus mail This stores messages that have triggered the Anti-Virus filter.
 - Junk mail This stores messages that have triggered the Anti-Spam filter.
 - Quarantine This stores messages that need to isolated, but which haven't triggered the Anti-Virus or Anti-Spam filter.
- You can create your own custom queues where messages that have been stopped can be stored.
- Once you have created a queue you can edit it at any time.
- You can use the supplied SurfControl dictionaries or create your own using the Dictionary Manager.
- The SurfControl Dictionaries cover the same type of content as the categories found within the Internet Threat Database.
- You can change the value of a word or phrase to fine-tune your filtering.


- With phrase value:
 - Increasing the value will increase filtering strength
 - Decreasing the value will decrease filtering strength
- Rather than creating a new dictionary, you can import a ready-made one from elsewhere. There are two ways in which you can import dictionaries into RiskFilter:
 - Import a SurfControl dictionary pack
 - Import a unicode text file
- Importing a unicode text file is an easy way to add large numbers of words and their scores to an existing dictionary, or create a new one.
- There are two ways of exporting Dictionaries:
 - As a SurfControl Dictionary pack (an XML file)
 - As a unicode file
- The policy module of RiskFilter supports infinite policy recursion, i.e. the global policy can include multilevel sub-policies.
- Once you have created a policy, you can edit it or delete it at any time.
- The supplied filters consist of an Anti-Virus Filter McAfee, Anti-Spam Filters Heuristics and LexiRules, Internet Threat Database Filter, General Content Filter, Advanced Content Filter, Message Attachment Filter, Content Guardian and Standard Disclaimer filter.
- Once you have added one of the following filters you will be unable to add another filter of the same type: Anti-Virus Agent - McAfee, Anti-Spam Agent - DFP, Anti-Spam Agent - Heuristics, Anti-Spam Agent - LexiRules and Standard Disclaimer.
- The Anti-Virus Agent filter is supplied with the product and enabled by default, so it will filter messages automatically without any prior modification.
- The Internet Threat Database Filter enables you to maximise message filtering by using SurfControl's database of 9 Million URLs. This enables you to apply a rule to a group of URLs rather than having to enter each one individually.
- A valid keyword expression is composed of keywords and logical operators.
- Multiple operators can be used in a single keyword expression, but multiple operator types are not allowed in a single dynamic keyword expression.
- The filtering criteria of Content Guardian consists of one or more filtering rule(s) which are made up of three parts: filtering target, matching condition, and filtering content.
- RiskFilter is pre-configured with the following dictionaries: Adult, Alcohol/Tobacco/Drugs, Arts/ Entertainment, Computing/Internet/hacking, Confidential, Finance, Gambling, Hate speech/Offensive, Job search, Medical/Healthcare, Shopping, Spam, Spam Misspellings, Sports, Travel and Violence/ Weapons.
- The Dictionary Threshold filter works by assigning each word a numeric value. It then checks to see how many words from the selected dictionaries appear within a message and adds up the total. If this value is greater than the value specified in the Dictionary Threshold filter, the filter will trigger.

Reports & Logs

e Reports and Logs tab	age 106
aster Report	age 108
essage Report	age 110
licy Report	age 111
rus Report	age 112
pam Report	age 113
onnection Report	age 114
stem Report	age 116
plated Messages	age 117
rus Messages	age 119
pam Messages	age 121
chived Messages	age 123
eferred Messages	age 127
ey Points	age 129



The Reports and Logs tab

This chapter explains how to run detailed reports on messages. From these you can learn about such things as the system status and message statistics. Log records keep information on mail circulation, system traffic, scanning results and the operating results of filters triggered. RiskFilter collects statistics and updates them on a real-time basis.

TERMINOLOGY USED

The following terminology is used in this chapter:

- RBL How many connections were from senders on the Real-Time Blacklist.
- RDNS How many connections were dropped due to RDNS failing to validate the reverse DNS lookup of the senders IP address.
- **SPF** How many connections were dropped due to failing the SPF check.

WHAT CAN BE CONFIGURED IN THE REPORTS AND LOGS TAB?

In this tab you can configure anything to do with the reporting and logging of e-mail use. RiskFilter can also record and report on traffic patterns and scan results

SurfContrøl'	System Settings Policy Manager Reports & Logs SurfControl RiskFilter - E-m
<u>Dashboard</u>	Reports & Logs
Master Report	SurfControl RiskFilter - E-mail Reports & Logs is designed to offer superior visibility into your e-mail system with detailed, easy-
Message Report	to-understand logs. Reports are created daily. You can review reports by month, day or hour. They give insight into e-mail usage and traffic patterns, scan results, and compliance with corporate e-mail policy. You can browse all logs, or query logs that match your search criteria
Virus Report	There are thirteen types of report available:
Spam Report	Dashboard: shows the status of the system and its services.
Connection Report System Report	Master Report: shows a summary of your e-mail traffic, including incoming, outgoing, spam, virus and policy violations.
Isolated Messages Virus Messages	Message Report: reports e-mail usage and traffic patterns through SurfControl RiskFilter - E-mail in detail. You can choose to view a daily report or an hourly report. It also lists the top ten heavy traffic users in terms of volume and size.
Spam Messages Archived Messages	Policy Report: reports any policy violations detected by SurfControl RiskFilter - E-mail filters (excluding Anti-Spam and Anti-Virus filters). It includes information about sender, receiver, filter type, filter actions taken and top 10 policy violations for inbound and outbound messages.

Figure 4 - 1 The Reports and Logs tab

Reports and Logs enables you to:

- Configure general messages
- · View reports on messages that have been isolated to different queues
- · View reports on messages that have violated policies.
- · View reports on messages that have been categorized as spam or virus.



DASHBOARD

RiskFilter enables you to query the status of all distributed RiskFilter servers, protected e-mail servers and LDAP servers via the dashboard on a real-time basis. At the same time, the dashboard presents a summary of statistical results for messages and connections in graphical format.



Server status monitoring

- Server The condition monitoring all processing modules of the SMTPD service, delivery service, policy service, Anti-Virus engine and Anti-Spam engine. When the status of the RiskFilter server is shown as off-line, you can use the Dashboard to find out which service is experiencing problems. Status is also shown as abnormal if the services have been restarted.
- **Mail server status** RiskFilter can monitor the status of all protected e-mail servers. You can check that the protected e-mail servers are working normally by the status display (online or unknown). This alerts you to possible protected e-mail server problems.
- LDAP server status RiskFilter can monitor all servers used for validation and importing of e-mail addresses. You can identify whether the LDAP servers are working normally by the status display (online or unknown).

Click **Refresh** to refresh the status display.



Note: RiskFilter supports distributed processing systems. You may monitor the status of each server within the distribution system in real time via the RiskFilter Console.



MASTER REPORT

The Master Report shows statistical results of all legitimate spam, virus and policy violation messages received and sent by RiskFilter. The results include the statistical results for all domains (in graphical format) and provide you with query functions.

- To query the statistical report of the current date for all domains in real time, click **Today's Report**.
- To view the statistical report of a certain period of time of a selected year, month and date for a certain domain, make respective selections from the drop-down list boxes at the top of the page. Click View Report to see a corresponding statistical report.

EXAMPLE: the following example shows the settings needed to query the statistical information from October 3rd to October 7th in 2005 for all domains.

Master Repo	rt				
		All descelar			
l	Domain:	All domains 🛛 👻			
L	Logs for:	Past 7 days 💌			
St	art Date:	May 💙 30 💙 20	2006 🔽		
E	nd Date:	June 🛛 🖌 5 😪 20	2006 🔽		
		View Report Toda	lay's Report		
			Master Report		
	la.	haved Massage Count		Outbound Massage Count	
	In	bound message Count		outbound message Count	
		🗖 Legi	gitimate 📕 Virus 🗕 Spam 📕 P	olicy	
•					

Figure 4 - 2 Querying Statistical Report of All Messages

QUERYING THE MASTER REPORT

Click Today's Report to view a report on todays logs.

To create a report on specified criteria:

- 1 Select Master Report from the Reports and Logs tab.
- 2 Select All domains from the Domain: list box.
- 3 Select **Specified date range** from the **Logs for:** list box.
- 4 Select the date that you want the report to start from: choose the month, day and year from the list boxes or click on the calendar icon to select a day on the calendar to automatically fill in these fields.
- 5 Select the date that you want the report to end: choose the month, day and year from the list boxes or click on the calendar icon to select a day on the calendar to automatically fill in these fields.



- 6 Click one of the following:
 - View Report Logs are compounded every day at various intervals. Selecting View Report will show a report based on the last time one of these updates took place.
 - **Today's Report** Selecting Today's Report will compute any existing log data immediately and show you Today's report based on this information.

The report should look something like this.



Figure 4 - 3 Querying Statistical Report of All months in 2004 for All domains

RiskFilter uses different collection criteria when collecting statistics for domains:

- All domains Statistics are collected based on the IP of the message source. All messages from the specified IP addresses or address range (the IP address list of internal e-mail server as listed in System Settings > Receive Settings > Relay Control) will be reported as outbound messages. All messages from IP addresses other than the ones on this list, will be reported as inbound messages.
- Report on separate domains Statistics are collected based on the domains of the message sender and recipient. Messages to or from specified domains (those included in 'Accept e-mail for relay to the following domains' as listed in System Settings > Receive Settings > Relay Control) will be reported on as respective domains.



MESSAGE REPORT

The Message Report includes information on the total number and size of all messages for all allowed messages going through RiskFilter. This includes inbound, outbound and messages that are sent both ways. The Message Report also automatically lists the top 10 users based on the number and size of allowed messages for inbound and outbound. There are two ways in which you can query this statistical information:

- Query the statistical information on allowed messages for the current date, or alternatively, a certain period of time for the selected year, month and date for a particular domain.
- Browse and query the RiskFilter message log for messages and the corresponding delivery information.



Figure 4 - 4 Message Report

QUERYING THE MESSAGE REPORT

You can perform the following tasks:

- **Message Log** View and download the log records of messages received. Specify a keyword such as Date, Time etc to find out whether an allowed message has been correctly received by RiskFilter.
- Delivery Log View and download the log records of messages delivered to the e-mail system by RiskFilter. Specify a keyword such as Date, Time etc., to query whether a message has been successfully delivered by RiskFilter.
- View Report First, specify criteria for a report by selecting items from the drop-down lists at the top of the page then click the View Report.
- Today's Report Shows you all messages since 12.00am this morning.



POLICY REPORT

The Policy Report provides statistical information on any policy violation messages detected by any of the five filters: General Content Filter, Advanced Content Filter, Message Attachment Filter, Content Guardian and Dictionary Threshold Filter. RiskFilter automatically lists the top 10 policy violations and the number of corresponding messages stopped by these filters.

QUERYING THE POLICY REPORT

There are two ways in which you can query these messages:

- Query these messages to find out when one of these filters was triggered. Details could include the current date, or alternatively, a certain period of time for the selected year, month and date.
- Policy Report Domain: All domains Logs for: Past 7 days Start Date: End Date Browse Log View Report Today's Report Policy Report Count 2006-5-31 006-6-1 -9-9003 -9-900 006-6 2006-(Date Inbound Outbound Date Inbound Outbound Total Total 0 0 Top 10 Policy Violations Count
- · Browse and query the corresponding policy logs with keywords.

Figure 4 - 5 Displaying statistical results in Policy Report



- **Browse Policy Logs** View and download the log records of messages that trigger any of the above types of filter. You can query the Date, Time etc. to retrieve records of policy violation messages.
- View report First, specify criteria for a report by selecting items from the drop-down lists at the top of the page then click View Report.
- Today's Report Shows you all messages since 12.00am this morning.



VIRUS REPORT

The Virus Report provides the statistical information on all messages containing viruses that have been scanned by the RiskFilter Anti-Virus engine. The system automatically lists the top 10 viruses and the number of virus messages scanned by the Anti-Virus engine.

QUERYING THE VIRUS REPORT

There are two ways in which you can query these messages:

- Query the scanned virus messages of the current date, or alternatively, a certain period of time for the selected year, month and date for a particular domain.
- Query the virus logs.

Virus Report							
Domain:	All domains	~					
Logs for:	Past 7 days	~					
Start Date:	May 💙 31 🔹	2006 🗸					
End Date:	June 🗸 6	2006 🗸					
	Browse Log	/iew Report	Today's Rep	oort			
		Virus	Report				
Count 2006-5-31	2006-6-1	2006- 6- 2 2006 - 1- 2	°- 9907 Date ■ Outbound	2006-6-4	2006-6-5	2006-6-6	
Date		Inbound		Outbound		Total	
2006 Jun 5		1		0		1	
Total		1		0		1	
1	Top 10 Viruses Count						
Encrypted Message					1		

Figure 4 - 6 Displaying statistical results in a Virus Report

- **Browse Log** View and download the log records of virus messages scanned and processed by the Anti-Virus engine. You can specify a keyword such as Date, Time etc, to retrieve records of virus messages.
- View report First, specify criteria for a report by selecting items from the drop-down lists at the top of the page then click View Report.
- Today's Report Shows you all messages since 12.00am this morning.



SPAM REPORT

The Spam Report provides statistical information on all spam messages caught by the Anti-Spam engine. RiskFilter automatically lists the top 10 spam recipients and the number of spam messages received by them.

QUERYING THE SPAM REPORT

There are two ways in which you can query these messages:

- Query spam messages that have been stopped on the current date, or alternatively, messages stopped over a certain period of time for the selected year, month and date for a particular domain.
- Btowse and query records of spam messages.

Spam Report						
Domain:	All domains	~				
Logs for:	Past 7 days	~				
Start Date:	May 🗸 31	2006 🗸				
End Date:	June 🗹 6	2006 🗸				
	Browse Log	View Report	Today's R	eport		
		Spar	n Report			
5						
4						
Ę 3						
ē,						
-						
1						
0						
2 2	-6-1	-6-2		-6-4	5-9-1	9-9-
-900	2006	2006	2006	2006	2006	2006
			Date			
		Inbour	nd 🗖 Outbound			
Date		Inbound		Outbound		Total
2006 Jun 5		5		0		5
Total		5		0		5
Top 1	Top 10 Spam Recipients Count					
wahaha@lasa.surfcontrol.	wahaha@lasa.surfcontrol.com 3					
gangli@lasa.surfcontrol.co	gangli@lasa.surfcontrol.com 1					
wuyaya@lasa.surfcontrol.c	om				1	

Figure 4 - 7 Displaying statistical results in a Spam Report

- Browse Log View and download the log records of spam messages caught and processed by the Anti-Spam engine. You can specify the keyword such as Date, Time etc., to retrieve records of spam messages.
- View Report First, specify criteria for a report by selecting items from the drop-down lists at the top of the page then click View Report.
- Today's Report Shows you all messages since 12.00am this morning.



CONNECTION REPORT

The Connection Report provides statistical information on connections made and released by RiskFilter. It includes connection data relating to real-time blacklist, block host, directory attack, reverse DNS lookup and connection limit, as well as attachment scanning, SPF and SMTP delay.

RiskFilter automatically lists the top 10 IP addresses accepted and rejected as well as the number of connections and the size of data sent through respective IP addresses.

QUERYING THE CONNECTION REPORT

There are two ways in which you can query the Connection report:

- Query the number of connections made and released on the current date, or alternatively, over a certain period of time for the selected year, month and date for a particular domain.
- · Use keywords to browse and retrieve records of connections.



Figure 4 - 8 Connection Report

- Browse Log View and download the records of connections. You can specify the keyword such as Release Date, Release Time etc., to retrieve records of Connection messages.
- View Report First, specify criteria for a report by selecting items from the drop-down lists at the top of the page then click View Report.
- Today's Report Shows you all messages since 12.00am this morning.

The report shows the following information:

• Total Connections - How many connections were made in the specified period.



- RBL How many of these connections were from blacklisted senders, listed in the RBL. This is set in System Settings> Receive Settings > Connection Control > RBL (Perform real-time black list (RBL) check).
- **Directory Attack** How many connections were categorized as directory attacks and dropped. This is set in **System Settings > Receive Settings > Directory Attack**.
- RDNS How many connections were dropped due to RDNS failing to validate the reverse DNS lookup of the senders IP address.
- **Connection Limit** How many connections were dropped because the connection limit was exceeded (for IP or For Server). This is set in **System Settings > Receive Settings > Connection Control**.
- Attachment How many connections were dropped/blocked because they violated the connection level Message Attachment policy. This is set in System Settings > Receive Settings > Message Control (Block messages with attachments of a specific type).
- SPF How many connections were dropped due to failing the SPF check. This is set in System Settings > Receive Settings > Relay Control > SPF Authentication Configuration.
- SMTP Delay How many connections were dropped due to the sending client starting the session before the SMTP greeting message was displayed. This is set in System Settings > Receive Settings > Connection Control > SMTP Greeting Delay.
- Block Host How many connections were from hosts listed in the Blacklist.



System Report

The System Report provides statistical information on the current status of RiskFilter, including detailed information on messages received, processed and delivered by the system to date and message queue usage.

System Report	
	SurfControl RiskFilter Server: e30.sdrf.com.au 💊
Current time:	Wednesday, October 12, 2005 10:11:03 AM EST
SurfControl RiskFilter start time:	Tuesday, October 11, 2005 1:28:34 AM EST
Last counter reset:	Wednesday, October 12, 2005 2:55:28 AM EST
Total Messages received lifetime to date:	53372
Total Messages processed lifetime to date:	53372
Messages delivered successfully since last counter reset:	2527
Messages bounced since last counter reset:	7
Messages in Queue:	0
Messages in deferred Queue	0
Message Queue Total Space:	4088 MB
Message Queue Used Space:	0 MB
Message Queue Available Space:	4088 MB
Deferred Message Queue Total Space:	4088 MB

Figure 4 - 9 System Report

- To Browse the Status of a Specific RiskFilter Server Select the RiskFilter server that you want to view from the RiskFilter Server drop-down list box. Click Refresh.
- Reset Counter Click Reset Counter to have the system reset the values of items as shown below:
 - Last counter reset
 - Messages delivered successfully since last counter reset
 - Messages bounced since last counter reset



ISOLATED MESSAGES

Isolated Messages archives all messages isolated by RiskFilter. This enables you to perform a variety of tasks on the messages which include: query, delete, deliver, forward, reprocess or download and save specified messages.

Isolated Messages						
This feature enables you to query isolated messages to view messages that match your criteria. Isolated messages are those which have been saved to the quarantine queue as well as all user-defined queues added in the Queue Manager. Use the Queue selection dialog below to query a specific queue.						
Queue:	quarantine 💌					
Domain:	All domains 🔽					
Messages for:	Past 24 hours					
Start Date:	October 😒 - 11 😒 - 2005 😒					
End Date:	October 👽 - 12 👽 - 2005 👽					
	View Messages					

Figure 4 - 10 Querying Isolated Messages Report

MANAGING ISOLATED MESSAGES

To query an Isolated Messages report:

- 1 Select Isolated Messages from the Reports and Logs tab.
- 2 Select the queue that you want to query from the **Queue** drop-down list box.
- 3 Select the domain name from the Domain drop-down list box. This list will show the default of All domains as well as any other domains that you have defined in System Settings > Receive Settings > Relay Control.
- 4 Select the query date from the **Messages for** drop-down list box. By default **Past 24 hours** is displayed. If you select a specified date range, the following query criteria will need to be selected:
 - The Start Date of the report
 - The End Date of the report
- 5 Click View Messages.
- 6 You will see all isolated messages that match the query criteria and their status in a new window. In this window you can:
 - Refresh the current page display by clicking Check New Messages.
 - Search with keywords such as Recipient, Sender in the selected queue.
 - Jump to a new page by specifying a page then clicking **Go**.

Isolated Messages - quarantine								
_	Check New Messages	Total M	essages 4 / Total Size 5.4KB	Se	nder 🔽		Search	
<u> </u>			Page 1 / Total Page 1			-		
	Sender	Recipient	Subject		Size	Date	Policy	
	eee2@in.com	eee2@in.com	<u>dadada</u>		1.3KB	2006/05/25 18:38:22	Isolate IN.COM	
	eee2@in.com	eee2@in.com	dadada		1.3KB	2006/05/25 16:25:20	Isolate IN.COM	

Figure 4 - 11 Isolated messages



- 7 To view a message, click the subject.
- 8 Select the message that you want to process.
- 9 You can process any of the messages archived in the isolated messages queue in any of the ways shown below:
 - **Delete** Delete the selected message.
 - Deliver Deliver the selected message.
 - Reprocess Release the selected message to the message queue for reprocessing. You can
 configure existing filter settings to reprocess an isolated message and deliver it to the back-end email system.
 - **Download** Download the selected message.
 - Empty Remove all messages in the isolated messages queue.
 - Forward Forward the selected message to a specified recipient. Enter their e-mail address into the field.



Caution: You can only forward one message at a time. If you enter more than one e-mail address, the message will not be forwarded.



VIRUS MESSAGES

Virus Messages archives all virus messages caught by RiskFilter. This enables you to perform a variety of tasks on the messages which include: query, delete, release, download, reprocess and forward specified messages.

Virus Messages							
This feature enables you to those which have been save	query virus infected messages to view messages that match your criteria. Virus infected messages are ed to the virusmail queue.						
Domain:	All domains 💌						
Messages for:	Past 24 hours						
Start Date:	October 👽 - 11 👽 - 2005 👽						
End Date:	October 👽 - 12 👽 - 2005 👽						
	View Messages						

Figure 4 - 12 Querying Virus Messages

MANAGING THE VIRUS MESSAGES

To query your Virus Messages:

- 1 Select Virus Messages from the Reports and Logs tab.
- 2 Select the domain name you want to query from the **Domain** drop-down list box. This list will show the default of **All domains** as well as any other domains that you have defined in **System Settings > Receive Settings > Relay Control**.
- 3 Select the query date from the Messages for drop-down list box. By default Past 24 hours is displayed. If you select a specified date range, the following query criteria will need to be selected:
 - The Start Date of the report
 - The End Date of the report

4 Click View Messages.

5 You will see all deferred messages that match the query criteria and their status in a new window.

Viru	Virus Messages						
						Sender 💌	Gaarch
	Check New Meccado	20	Total	Messages 54 / Total Size 276.4KB			Usaich
	CHECK NEW MESSage			Page 1 / Total Page 2			<u>Next></u> Last>>
	Sender	Recip	ient	Subject	Size	Date 🖟	Policy
	testsmg186@225.com	225smg	g185@183.com	Virus Scanner Test#15	2.2KB	2005/10/13 01:21:18	Anti-Virus Agent - McAfee
	testsmg121@225.com	225smg	g120@183.com	Virus Test 4 - Eicar.com.bd	2.3KB	2005/10/13 01:21:12	Anti-Virus Agent - McAfee
	testsmg115@225.com	225smg	g114@183.com	Virus Test 6 - eicarcom2.zip	2.6KB	2005/10/13 01:21:12	Anti-Virus Agent - McAfee
	testsmg114@225.com	225smg	g113@183.com	Virus Test 5 - eicar com.zip	2.5KB	2005/10/13 01:21:12	Anti-Virus Agent - McAfee
	Top Next> Last>>						
De	lete Deliver F	Reproce	ss Dowr	load Empty Forward			
							Jump To Page 1 Go
						Messa	iges Per Page 50 GO

Figure 4 - 13 The Virus Messages list

Refresh the current page display by clicking Check New Messages.



- Search with keywords such as Recipient and Sender.
- Jump to a new page by specifying a page then clicking **Go**.
- 6 To view a message click the hyper-linked subject.

Spam Messages						
Sender:	<test@totot.com></test@totot.com>	1				
Recipient:	<shorne@test.com></shorne@test.com>					
From:	<administrator@sydmail1.com></administrator@sydmail1.com>]				
To:	<administrator@sydmail1.com></administrator@sydmail1.com>					
Cc:	<administrator@sydmail1.com></administrator@sydmail1.com>					
Sent Date:	Tue Apr 26 16:54:05 CST 2005					
Subject:	Knock-out round, your final chance to be a winner					
Header:	Show headers					
Delete Deliver	Reprocess White List Not Spam Download Forward					
HTML Format	< <previous next="">> Back</previous>					
Hi there Karl, There is one more week left for you to take part in the Ready to Rumble Promotion this April at Jackpot City! We have already given away 300 prizes this month but this match is not over yet.						

Figure 4 - 14 An Archived message

7 Select the message that you want to process.

Sender	Recipient
testsmg186@225.com	225smg185@183.com
testsmg121@225.com	225smg120@183.com
testsmg115@225.com	225smg114@183.com

- 8 You can process any of the messages archived in the virus messages queue in any of the ways shown below:
 - **Delete** Delete the selected message.
 - **Deliver** Deliver the selected message.
 - **Reprocess** Release the selected message to the message queue for reprocessing. You can configure existing filter settings to reprocess a virus message and deliver it to the e-mail system.
 - **Download** Download the selected message.
 - Empty Remove all messages in the virus messages queue.
 - Forward Forward the selected message to a specified recipient. Enter their e-mail address into the field.



Caution: You can only forward one message at a time. If you enter more than one e-mail address, the message will not be forwarded.



SPAM MESSAGES

Spam Messages archives all spam messages caught by RiskFilter. This enables you to perform a variety of tasks on the messages which include: query, delete, release, download, reprocess, add to a white list, specify as 'not spam' and forward specified messages.

Spam Messages		
This feature enables you to been saved to the junkmail	- query spam messages to view messages that match your criteria. Spam messag queue.	es are those which have
Domain:	All domains 💌	
Messages for:	Past 24 hours 👻	
Start Date:	Past 24 hours _ 2005	
End Date:	Yesterday _ 2005 😪	
	Past 7 days Past 30 days	
	Specified date range	
@ 1999-2005 SurfCo		

Figure 4 - 15 Querying Spam Messages Report

MANAGING SPAM MESSAGES

To manage your spam messages:

- 1 Select Spam Messages from the Reports and Logs tab.
- 2 Select the domain name you want to query from the **Domain** drop-down list box. This list will show the default of **All domains** as well as any other domains that you have defined in **System Settings > Receive Settings > Relay Control**.
- 3 Select the query date from the **Messages for** drop-down list box. By default **Past 24 hours** is displayed. If you select a specified date range, the following query criteria will need to be selected:
 - The Start Date of the report.
 - The End Date of the report.
- 4 Click View Messages.
- 5 You will see all deferred messages that match the query criteria and their status in a new window. In this window you can:
 - Refresh the current page display by clicking Check New Messages.
 - Search with keywords such as Recipient, Sender in the Deferred message queue.
 - Jump to a new page by specifying a page then clicking **Go**.
 - Specify how many messages you want to be viewed on each page at a time.



6 To view a message click the subject.

Spam Messa	ges			
Sender:	<test@totot.com></test@totot.com>			
Recipient:	<shome@test.com></shome@test.com>			
From:	«administrator@sydmail1.com»			
To:	<administrator@sydmail1.com></administrator@sydmail1.com>			
Cc:	<administrator@sydmail1.com></administrator@sydmail1.com>			
Sent Date:	Tue Apr 26 16:54:05 CST 2005			
Subject:	Knock-out round, your final chance to be a winner			
Header:	Show headers			
Delete Deli	ver Reprocess White List Not Spam Download Forward			
HTML Format	< <previous next="">> Back</previous>			
Hi there Varl				
There is of Ready to Re have alread match is no	ne more week left for you to take part in the mmble Promotion this April at Jackpot City! We dy given away 300 prizes this month but this at over yet.			
Be part of the winnings at Jackpot City this week and you could be the lucky winner who takes howe 5,000 casino credits in the final Knock-out Round! Jackpot City is also sending one lucky winner to an exhilarating boxing even worth \$10,000 of their choice!				

Figure 4 - 16 Viewing a Spam message

7 Select the message that you want to process.

Sender	Recipient
testsmg186@225.com	225smg185@183.com
testsmg121@225.com	225smg120@183.com
testsmg115@225.com	225smg114@183.com

- 8 You can process any of the messages archived in the virus messages queue in any of the ways shown below:
 - **Delete** Delete the selected message.
 - **Deliver** Deliver the selected message.
 - **Reprocess** Release the selected message to the message queue for reprocessing. You can configure existing filter settings to reprocess a virus message and deliver it to the e-mail system.
 - White List Add the sender of the selected message (usually mistakenly judged to be a spam message) to the White List. See White List on page 39 for details on how to do this.
 - **Not Spam** Send the selected message that has been mistakenly judged to be a spam message by RiskFilter, to the spam message analysis center of SurfControl.
 - **Download** Download the selected message.
 - Empty Remove all messages in the virus messages queue.
 - Forward Forward the selected message to a specified recipient. Enter their e-mail address into the field.



Caution: You can only forward one message at a time. If you enter more than one e-mail address, the message will not be forwarded.



ARCHIVED MESSAGES

Archived Messages archives all messages (including all virus, spam, policy violation and allowed messages) received by RiskFilter. This enables you to perform a variety of tasks on the messages.

Archived Messages					
This feature enables you to	query archived messages to view messages that match your criteria.				
Domain:	All domains 💌				
Messages for:	Past 24 hours				
Start Date:	October 🔽 - 11 🔽 - 2005 🔽				
End Date:	October 🔽 - 12 🔽 - 2005 🔽				
Sender:	*				
Recipient:	*				
	Support wildcard e.g. *@SurfControl.com * means all messages				
	Export Messages Reprocess Messages View Messages				

Figure 4 - 17 The Archived Messages screen

MANAGING ARCHIVED MESSAGES

Use the Archive Messages screen to query the database and manage messages of a particular type.

To manage these messages:

- 1 Select Archived Messages from the Reports and Logs tab.
- 2 Select the domain name you want to query from the **Domain** drop-down list box. This list will show the default of **All domains** as well as any other domains that you have defined in **System Settings > Receive Settings > Relay Control**.
- 3 Select the query date from the **Messages for** drop-downlist box. By default **Past 24 hours** is displayed. If you select a specified date range, the following query criteria will need to be selected:
 - The Start Date of the report.
 - The End Date of the report.
- 4 You have the following options:
 - **Export Messages** Downloads the archived messages that match the query criteria. This will be an "Export Messages" zip file containing .eml files.
 - **Reprocess Messages** Reprocesses all the archived messages that match the query criteria. This will re-deliver the "Archived Messages".
 - View Messages Shows spam messages that match the query criteria in a new window, as shown. Refresh the current page display by clicking **Check New Messages**, or search with keywords such as Recipient/Sender, Subject and Policy in the isolated messages database.



Export Messages

You might want to download all the messages in the Archive, or just messages of a particular type, in order to perform particular actions on them.

To export messages:

- 1 Select Archived Messages from the Reports and Logs tab.
- 2 Use this screen to specify the type of messages that you are interested in (see **Managing Archived Messages on page 123**).
- 3 Click **Export Messages**. You may see a message stating: 'Downloading...If your download does not begin automatically click <u>here</u>' If this is the case click the link.
- 4 You will see a File Download dialog box where you can select:
 - **Open** View the contents of the Zip file containing the Exported Messages.
 - **Save** Save it to your system.

File Dov	vnload 🛛 🔀
Do you	u want to open or save this file?
Q	Name: 2005-10-12.zip Type: WinZip File From: lasa Open Save Cancel
1	While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. <u>What's the risk?</u>

- 5 A Download complete dialog box is displayed where you can select:
 - **Open** Open the zip file containing the downloaded messages.
 - Open Folder Open the directory where the zip file has been downloaded to.
 - **Close** Close the dialog and return to the Archived Messages screen.

Download complete					
Downle	oad Complete				
Saved: 2005-10-12.zip fro	om lasa				
Downloaded:	1.88 KB in 1 sec				
Download to:	C:\Documents and Se\2005-10-12.zip				
Transfer rate:	1.88 KB/Sec				
🔄 Close this dialo	g box when download completes				
	Open Open Folder Close				



Reprocess Messages

Reprocessing messages enables you to resend all messages to the Archive folder. This would be useful in the event, for example, of a mail server failing and messages not being delivered. Clicking **Reprocess Messages** will resend all of the messages. You could also specify messages of a certain type then ask RiskFilter to resend all messages that match this criteria.

To reprocess messages:

- 1 Select Archived Messages from the Reports and Logs tab.
- 2 Use this screen to specify the type of messages that you are interested in (See Managing Archived Messages on page 123).
- 3 Click Reprocess Messages.
- 4 Click **OK** in the confirmation dialog that follows. The messages will be resent to the Archive Queue.



Note: If the messages already exist in the Archive Queue you will see that it now contains two copies of each message you reprocessed.

View Messages

Clicking **View Messages** enables you to see a list of all of the messages in the Archive Messages Queue. This enables you to process single messages as well as see what messages have been collected.

To view messages:

- 1 Select Archived Messages from the Reports and Logs tab.
- 2 Use this screen to specify the type of messages that you are interested in. See **Managing Archived Messages on page 123** for more details.
- 3 Click View Messages.
- 4 You will see all archived messages that match the query criteria and their status. In this window you can:
 - Refresh the current page display by clicking Check New Messages.
 - Search with keywords such as Recipient, Sender in the Deferred message queue.
 - Jump to a new page by specifying a page then clicking **Go**.
 - Specifying how many messages you want to be viewed on each page at a time.

Arc	hived Messages				
			S	ender 💌	
		Total M	lessages 3 / Total Size 33.4KB		Search
	Check New Messages	3	Page 1 / Total Page 1		
	Sender	Recipient	Subject	Size	Date 🖏
	hzbbax@excite.com	stiletto5@pellfrisc	Your Body pheromone	1.8KB	2005/07/21 19:17:03
	8danny@absolutemoti	pjackson@pellfrisch	поможем продать Ва	5.2KB	2005/07/21 11:20:26
	bounce-alq1cjmgi8fa	sward@pellfrischman	Vall Street Breaking News In Red H	26.3KB	2005/07/21 07:28:43
					Top
Dei	liver Reprocess	Black List Spa	m Download Forward		
				Jump	To Page 1 Go
				Messages	Per Page 5005 00

Figure 4 - 18 Archived messages



- 5 Refresh the current page display by clicking **Check New Messages**, or search with keywords such as Recipient, Sender, Subject and Policy.
- 6 Select the check box alongside the message that you want to process.

Sender	Recipient
testsmg186@225.com	225smg185@183.com
testsmg121@225.com	225smg120@183.com
testsmg115@225.com	225smg114@183.com

Figure 4 - 19 Select the check box alongside the message

- 7 You can process any of the messages archived in the virus messages queue in any of the ways shown below:
 - **Deliver** Deliver the selected message.
 - **Reprocess** Release the selected message to the message queue for reprocessing. You can configure existing filter settings to reprocess a virus message and deliver it to the e-mail system.
 - **Black List** Add the sender of the selected message to the blacklist (see Black List on page 37 for more details).
 - Spam Send the selected archived message to the spam message analysis center of SurfControl
 - **Download** Download the message.
 - Forward Forward the selected message to a specified recipient. Enter their e-mail address into the field.



Caution: You can only forward one message at a time. If you enter more than one e-mail address, the message will not be forwarded.



DEFERRED MESSAGES

Deferred Messages is used to store all messages for later delivery, for example in the event of an e-mail server crashing. RiskFilter E-mail will enable you to query, delete, retry, download, empty and forward specified messages.

Deferred Messages				
This feature enables you to query deferred messages to view messages that match your criteria.				
Server:	e30.sdrf.com.au 💌			
Messages for:	Past 24 hours			
Start Date:	October 🔽 - 11 🔽 - 2005 🔽			
End Date:	October 👽 - 12 👽 - 2005 👽			
	View Messages			

Figure 4 - 20 Querying Deferred Messages

QUERYING DEFERRED MESSAGES

To query Deferred Messages:

- 1 Select **Deferred Messages** from the **Reports and Logs** tab.
- 2 Select the domain you want to query from the **Domain** drop-down list box. This list will show any domains that you have defined in **System Settings > Receive Settings > Relay Control**.
- 3 Select the query date from the **Messages for** drop-down list box. By default **Past 24 hours** is displayed. If you select a specified date range, the following query criteria will need to be selected:
 - The Start Date of the report.
 - The End Date of the report.
 - Click View Messages.
- 4 You will see all deferred messages that match the query criteria and their status in a new window. In this window you can:
 - Refresh the current page display by clicking Check New Messages.
 - Search with keywords such as Recipient, Sender in the Deferred message queue.
 - Jump to a new page by specifying a page then clicking **Go**.
 - Specify how many messages you want to be viewed on each page at a time.

Deferr	ed Messages	5							
Ch	eck New Message	es	Total Messa Page (ges 0 / Total Size) / Total Page 0	08	Send	ler 💌		Search
	Sender	Recipient	Size	Date₿	Retry Date		Retry T	imes	Status
									Top
Delete	Retry Dov	vnload Empty	Forward						
								Jump To F	Page 0 Go
								Messages Per F	Page 50 Go

Figure 4 - 21 Deferred Messages screen



5 To view a message click the subject.

Spam Message	S			
Sender:	<test@totot.com></test@totot.com>			
Recipient:	<shorne@test.com></shorne@test.com>			
From:	<administrator@sydmail1.com></administrator@sydmail1.com>			
To:	<administrator@sydmail1.com></administrator@sydmail1.com>			
Cc:	<administrator@sydmail1.com></administrator@sydmail1.com>			
Sent Date:	Tue Apr 26 16:54:05 CST 2005			
Subject:	Knock-out round, your final chance to be a winner			
Header:	Show headers			
Delete Deliver	Reprocess White List Not Spam Download Forward			
HTML Format	< <previous next="">> Back</previous>			
Hi there Karl, There is one more week left for you to take part in the Ready to Rumble Promotion this April at Jackpot City! We have already given away 300 prizes this month but this match is not over yet.				

Figure 4 - 22 An Archived message

6 Select the message that you want to process.

Sender	Recipient
testsmg186@225.com	225smg185@183.com
testsmg121@225.com	225smg120@183.com
testsmg115@225.com	225smg114@183.com

Figure 4 - 23 Select the check box alongside the message

- 7 You can process all deferred messages as follows:
 - **Delete** Delete the selected deferred message.
 - **Retry** Try to redeliver the selected deferred message.
 - Empty Remove all messages in the Deferred messages queue.
 - **Download** Download the selected deferred message.
 - Forward Forward the selected message to a specified recipient. Enter their e-mail address into the field.



Caution: You can only forward one message at a time. If you enter more than one e-mail address, the message will not be forwarded.



KEY POINTS

The following list is a summary of the main points covered in Chapter 4. Use this list as a quick reminder of what you can do within the Reports and Logs tab:

- RiskFilter enables you to query the status of all distributed RiskFilter servers, protected e-mail servers and LDAP servers via the Dashboard on a real-time basis.
- When the status of the RiskFilter server is shown as off-line, you can use the Dashboard to find out which service is experiencing problems.
- RiskFilter can monitor the status of all protected e-mail servers and all servers used for validation and importing of e-mail addresses. You can identify whether the LDAP servers are working normally by the status display (online or unknown) in the Dashboard.
- RiskFilter supports distributed processing systems. You may monitor the status of each server within the distribution system in real time via the RiskFilter Console.
- The Master Report shows statistical results of all legitimate spam, virus and policy violation messages received and sent by RiskFilter.
- Logs are compounded every day at various intervals. You can, however, ask RiskFilter to compute any existing log data immediately and show you Today's report based on this information.
- The Message Report includes information on the total number and size of all messages for all allowed messages going through RiskFilter. This includes inbound, outbound and messages that are sent both ways.
- The Policy Report provides statistical information on any policy violation messages detected by any of the five filters: General Content Filter, Advanced Content Filter, Message Attachment Filter, Content Guardian and Dictionary Threshold Filter. The statistical results of Anti-Spam and Anti-Virus filters are not included in this report.
- The Virus Report provides the statistical information on all messages containing viruses that have been scanned by the RiskFilter Anti-Virus engine.
- The Spam Report provides statistical information on all spam messages caught by the Anti-Spam engine.
- The Connection Report provides statistical information on connections made and released by RiskFilter. It includes connection data relating to real-time blacklist, block host, directory attack, reverse DNS lookup and connection limit, as well as attachment scanning, SPF and SMTP delay.
- The System Report provides statistical information on the current status of RiskFilter, including detailed information on messages received, processed and delivered by the system to date and message queue usage.
- Virus Messages archives all virus messages caught by RiskFilter. This enables you to perform a variety of tasks on the messages which include: query, delete, release, download, reprocess and forward specified messages.
- Isolated Messages archives all messages isolated by RiskFilter. This enables you to perform a variety
 of tasks on the messages which include: query, delete, deliver, forward, reprocess or download and
 save specified messages.



- Spam Messages archives all spam messages caught by RiskFilter. This enables you to perform a variety of tasks on the messages which include: query, delete, release, download, reprocess, add to a white list, specify as 'not spam' and forward specified messages.
- Archived Messages archives all messages (including all virus, spam, policy violation and allowed messages) received by RiskFilter. This enables you to perform a variety of tasks on the messages.
- Reprocessing messages enables you to resend all messages to the Archive folder.
- You can process single messages as well as see what messages have been collected.
- The Deferred message queue is used to store all messages for later delivery, for example in the event of an e-mail server crashing.

RiskFilter System Management Console

Overview	. page 132
The Webmin Tab	. page 134
The System Tab	. page 138
The RiskFilter Tab	. page 148
Key Points	. page 155



OVERVIEW

The RiskFilter System Management Console enables you to configure the RiskFilter appliance and its interaction with the surrounding network. You can also use the RiskFilter System Management Console to manage this appliance's interaction with the network, and to monitor system resources.

WHAT CAN BE CONFIGURED WITH THE SYSTEM MANAGEMENT CONSOLE?

With the RiskFilter Management Console you can:

- Use IP Access Control to only allow access to those IP addresses that you trust. This will prevent unauthorized access being gained by anyone who guesses your password.
- Make changes to the language that titles, prompts and messages etc will be displayed in within the RiskFilter appliance interfaces.
- Make network specific changes such as adding RiskFilter Management Console servers and specifying which IP addresses and port RiskFilter Management Console will bind to.
- Keep records of the various actions taken by administrators of the RiskFilter Management Console server.
- Check things like historic system settings and running processes.
- · Change passwords.



Figure 5 - 1 The RiskFilter System Management Console

The System Management Console consists of three tabs:

- Webmin
- System
- RiskFilter

See the following sections for detailed information on what can be configured with these tabs.



ACCESSING THE RISKFILTER SYSTEM MANAGEMENT CONSOLE

To open the RiskFilter System Management Console:

1 Open a web browser and enter:

https://<hostname_or_ipaddress>:10000/

where '<hostname_or_ipaddress> is the name or IP address of your RiskFilter appliance.

- 2 At the RiskFilter Management Console login page enter that username and password. The default username and password are:
 - Username = rfmngr
 - Password = \$rfmngr\$
- 3 Click Login.

THE RFMNGR ACCOUNT

The rfmngr account enables you to configure the SurfControl software on the appliance by giving you three tabs, each containing modules relating to some aspect of RiskFilter.

The default username and password for the rfmngr account and thus the RiskFilter System Management Console is:

- Username = rfmngr
- **Password =** \$rfmngr\$



Note: When you start to configure RiskFilter you need to update the SurfControl OS and RiskFilter software as detailed in the Starter Guide.

THE WEBMIN TAB

This chapter explains how to use the Webmin tab to manage the RiskFilter System Management console and its connections.

WHAT CAN BE CONFIGURED IN THE WEBMIN TAB?

The Webmin tab enables you to:

- Generate reports on actions carried out by users within any of the modules, such as changing passwords, booting up/shutting down the computer or any configuration within the console.
- Access modules to manage IP access, the language of messages from Webmin, ports and addresses, logging and proxy servers.
- Monitor multiple RiskFilter appliances wthout having to remember the password for each appliance.

SurfControl		Webmin System	RiskFilter	RiskFilter System Management (
Webmin				
		×		
	Webmin Actions Log	Webmin Configuration	Webmin Servers II	ndex

Figure 5 - 2 Webmin

In this tab you have access to the following modules:

- Webmin Actions Log
- Webmin Configuration
- Webmin Servers Index

See the following sections for detailed information on what can be configured with these modules:



WEBMIN ACTIONS LOG

Use the Webmin Actions Log to generate reports on actions carried out by users within any of the modules such as changing passwords, booting up and shutting down the computer and configuration issues. You can search for actions by specifying the user, the module and the time that actions took place:

Webmin Actions Log		
Note - Logging of file changes is not currently enabled, so the details of logged actions will not include changed files or commands executed.		
Search the Webmin log for actions		
By any user By user Imngr By any user except		
 In any module In module Bootup and Shutdown 		
 At any time For today only 		
Between / Jan V/ and / Jan V/		
Search		

Figure 5 - 3 Specifying criteria

Once you have specified the criteria you want to search for, click **Search** to start the search.

WEBMIN CONFIGURATION

Select Webmin Configuration from the Webmin tab:

Webmin Configuration			
IP Access Control	Ports and Addresses	Logging	Proxy Servers
Language			

Figure 5 - 4 The Webmin Configuration Screen

IP access control

Use IP Access Control to only allow access to the appliance from IP addresses that you trust. This helps prevent access being gained by anyone who guesses your password. The default setting is 'Allow from all addresses' in order that RiskFilter will allow access 'out of the box'. For security reasons we strongly recommend that you change this setting as soon as possible.

To use IP access control:

- 1 Select IP Access Control from the Webmin Configuration screen.
- 2 Select Only allow from listed addresses.
- 3 This will enable the edit pane on the right. Enter the IP addresses of all machines that you want to be able to access the RiskFilter System Management Console server.
- 4 Click Save.



Language

This is the language that titles, prompts etc will be displayed in within the RiskFilter appliance interfaces. To change the language.

- 1 Select Language from the Webmin Configuration screen.
- 2 Choose a language from the **Display in Language** drop-down list box.
- 3 Click **Change Language** to apply these settings.

Ports and Addresses

You can specify which IP addresses and port the RiskFilter System Management Console will bind to. This is useful if you want to have two interfaces on the machine. For example, you could have RiskFilter on a public network. One interface could be a public one yet the other can be on a private network. Setting up RiskFilter to only bind to the private network which will prevent access by the general public. By default, RiskFilter System Management Console runs on port 10000 but this can be changed to help hide it. Acceptable values for port numbers are between 1024 and 65356.

To specify ports and addresses:

- 1 Select Ports and Addresses from the Webmin Configuration screen.
- 2 Select how you want the RiskFilter System Management Console to bind from the drop-down list box in the **Ports and Addresses** screen that follows.
- 3 Click Save.

Logging

Webmin can keep records of changes made within the RiskFilter System Management Console.

To set up logging:

- 1 Select Logging from the Webmin Configuration screen.
- 2 Specify the actions you want to be logged:
 - · Log resolved hostnames Provide a hostname rather than just the IP address of the client .
 - Use combined log format (including referrer and user agent) Include the same information as the common log format with the addition of the referral field and the user_agent field:
 - Referrer gives the site that the client reports as having been referred from.
 - User-Agent the identifying information from the client browser.
 - **Clear logfiles every ... hours** Once a log file has been stored for the specified time it will be deleted. To keep logs for your records, include the Webmin log in your system backup process.
 - Log actions by all users Log anyone who configures the System Management Console.
 - Only log actions by Enter the names of the administrator/s that you want the Webmin to log.
 - Log actions in all modules Any activity taking place in any module of RiskFilter System Management Console will be logged.
 - Only log actions in Only the selected modules will be logged.
 - Log changes made to files by each action Any file change made will be logged. This can lead to extensive log files being created so available disk-space is crucial. Select **Enable logging**.
- 3 Once you have entered all of your logging details click **Save**.



Proxy Servers

The RiskFilter System Management Console needs to connect to the Internet to operate correctly. If you use a proxy server to access web and FTP sites on the Internet you need to tell Webmin about these machines:



Caution: Proxy Server authentication is not supported in this release of RiskFilter.

- HTTP proxy This is the proxy server used for HTTP server requests and should be in URL format. For example: <u>http://hello.com:100</u>
- FTP proxy This is the proxy server used for ftp server requests and should be in URL format. For example: <u>http://hello.com:100</u>
- No proxy for This lists servers that you want to connect to the Internet, without using the proxy. Use a comma, ',' and a space to separate more than one server.
 For example: Messagesoft.com, surfcontrol.com.

WEBMIN SERVERS INDEX

This feature is only relevent if you have several RiskFilter appliances.

The Webmin Servers Index enables you to monitor multiple RiskFilter appliances without you having to remember the password for each appliance.

EXAMPLE: In a master/slave cluster configuration all of the slaves could be added to the Webmin Servers index of the Master's webmin console. This would allow a single point of entry for the monitoring of all the servers within the cluster.

Adding Webmin Servers

You can add servers to the Webmin Servers Index using the Webmin Servers Index module.

To add servers:

- 1 Select Webmin Servers Index in the Webmin.
- 2 In the Webmin Servers screen select **Register a new server**.
- 3 Enter your server details and click **Save**.

THE SYSTEM TAB

This chapter explains how to use the System tab for operating system level configuration. You can also use this tab to monitor system processes and resources.

WHAT CAN BE CONFIGURED IN THE SYSTEM TAB?

The System tab enables you to:

- Instantly reboot or shut down the system.
- · Change the password of the rfmngr account.
- · View real time and historic monitors of system usage.
- · Set up dynamic routing to preserve ipv4 source addresses.



Figure 5 - 5 The System tab

In this tab you have access to the following modules:

- Bootup and Shutdown
- Change Passwords
- Historic System Statistics
- Multi Gateway Policy Routing
- Network Configuration

See the following sections for detailed information on what can be configured with these modules:



BOOTUP AND SHUTDOWN

Use the Bootup and Shutdown screen to immediately reboot or shut down the system by clicking the relevant button:

Bootup and Shutdown		
Reboot System	Click on this button to immediately reboot the system. All currently logged in users will be disconnected and all services will be re- started.	
Shut Down System	Click on this button to immediately shut down the system. All services will be stopped, all users disconnected and the system powered off (if your hardware supports it).	

Figure 5 - 6 The Bootup and Shutdown screen



Note: As soon as you click either of these buttons, all users will be disconnected from the system and the RiskFilter appliance will stop processing mail.

CHANGE PASSWORDS

You can use the Change Password screen to change the password of the rfmngr account.

To change the password:

- 1 Select Change Passwords in the System tab.
- 2 Enter a new password into the 'New Password' field. Re-enter the password into the 'New Password (again)' field.
- 3 Click **Clear Form** if you want to remove everything that you have entered.
- 4 Click Change.

HISTORIC SYSTEM STATISTICS

This enables you to view real time and historic monitors of system usage. This screen also displays the following modules:

- · CPU Shows the CPU load in a graphical format
- Io Shows loopback network activity in a graphical format
- · Users Shows how many users are logged into a UNIX shell
- Custom Set up and monitor a custom monitor
- eth0 Shows network activity on eth0
- **Disk** Shows disk usage by partition
- **firewall** Shows firewall activity
- eth 1 Shows network activity on eth1
- Configure modules Add or upgrade the modules
- Memory Displays memory usage in a graphical format
- · Process Shows the system process count


MULTI GATEWAY POLICY ROUTING

This module sets up dynamic routing to preserve ipv4 source addresses.



Caution: This should only be used if you are using NAT on your mail servers to forward mail to RiskFilter.

Multi Gateway Policy Routng enables you to override the default gateway setting in your routing table. Connections forwarded to RiskFilter will have their packets routed back through the source's configured gateway. This is needed if these connections are from multiple mail servers which do not perfom SNAT packet modifications. With this enabled, RiskFilter is able to see the original source of a forwarded connection and route packets back through this gateway.

Multi-Gateway Policy Routing must have mail server(s) that support iptables, so that emails can be relayed to RiskFilter before being forwarded.

To set up Multi Gateway Policy Routing:

1 Select Multi Gateway Policy Routing in the System tab.

Multi-Gateway Policy Routing						
Configured Gateways						
Interface	Ethernet (MAC) Address IP Address					
Configure a new Gateway						
Interface	Ethernet (MAC) Address	IP Address				
ethû 🛩		Add				

Figure 5 - 7 The Multi-Gateway Policy Routing screen

- 2 Select an **Interface** from the drop-down list box.
- 3 Enter the MAC address of the Gateway into the Ethernet (MAC) address field.
- 4 Enter the IP address of the Gateway into the IP Address field.
- 5 Click Add.



Note: To test RiskFilter, run this command on the mail server: iptables -A PREROUTING -t nat -p tcp -m tcp ! -s RF-IP --dport 25 -j DNAT. To use this feature, you MUST run this command on the mail server.



NETWORK CONFIGURATION

The Network Configuration tab enables you to specify how the RiskFilter System Management Console server connects and interacts with the network:

Network Configuration			
Network Interfaces	Routing and Gateways	التا عامل 200 الالکی شور الله الله DNS Client	21118 10.2124 10.2126 10.2117 Host Addresses
Click t Apply Configuration after a Webrr	his button to activate the current bool reboot. Warning - this may make yo in.	t-time interface and routing se our system inaccessible via th	ttings, as they normally would be e network, and cut off access to

Figure 5 - 8 The Network Configuration screen

Network Interfaces

You can specify what network interfaces are activated at Boot Time in the Network Interfaces screen:

Vetworl	etwork Interfaces						
Interface	es Active Now						
Name	Туре	IP Address	Netmask		Status		
eth0	Ethernet	192.168.86.2	255.255.2	55.0	Up		
	-		127.0.0.1 255.0.0		TT		
	Loopback	127.0.0.1	255.0.0.0		Up		
lo Interface Add a new	Loopback es Activated at	127.0.0.1 Boot Time	255.0.0.0		Up		
lo Interface Add a new Name	Loopback es Activated at interface Type	I27.0.0.1 Boot Time IP Address	255.0.0.0	Activate at l	Op Doot?		
lo Interface Add a new Name eth0	Loopback es Activated at interface Type Ethernet	I27.0.0.1 Boot Time IP Address 192.168.86.2	255.0.00 255.0.00 Netmask 255.255.255.0	Activate at l Yes	Up Doot?		
lo Interface Add a new Name eth0 eth1	Loopback es Activated at interface Type Ethernet Ethernet	I27.0.0.1 Boot Time IP Address 192.168.86.2 192.168.86.121	255.0.00 Netmask 255.255.255.0 255.255.255.0	Activate at l Yes No	Up Doot?		

Figure 5 - 9 The Network Interfaces screen

- Interfaces Active Now A list of interfaces that are currently up and running. This is the same information as that gained when running <code>ipconfig -a</code> from the command line.
- Interfaces Activated at Boot Time A list of interfaces that are configured permanently on the system. These can be brought up optionally at boot up.
- Add a new interface Enables you to add your own interfaces (this is only available for interfaces activated at Boot Time).

Multi-NIC configuration in RiskFilter

You can use Webmin to set up a multi NIC environment. Once this is done, both IPs can be used to access the System Management console, the Management Console, the MTA and all other services. The following scenarios are possible.

RiskFilter between two networks. You can set up RiskFilter between two networks, for example between the user network and the DMZ (Demilitarized: Zone):



Figure 5 - 10 RiskFilter between two networks

- Network 1 A network in which clients send e-mail to RiskFilter. This network could be blocked for access to the System Management Console and the Management Console via a firewall. This is connected to the eth0 NIC.
- **Network 2** The network where the internal servers lie. This network holds the mail servers and RiskFilter administration clients. This is connected to the eth1 NIC.
- **RiskFilter** Your RiskFilter appliance comes with eth0 configured. You set up the second NIC (eth1 in the above example) as follows.

Setting up additional NICs

To select up additional NICs

- 1 Select the Network Configuration module in the System tab.
- 2 Select Network Interfaces.
- 3 Select the Add a new interface link in the Interfaces Activated at Boot Time section.
- 4 In the **Create Bootup Interface** screen add the following information:
 - Enter a **Name** for the interface (in Figure 5 10 we have used eth1).
 - Enter an IP Address
 - Enter a Netmask address.
 - Enter a MTU setting (SurfControl recommend using 1500).
 - Enter a **Broadcast** address.
 - Leave the Activate at boot? at it's default Yes setting.
 - Click Create.



Create Bootup Interface					
Boot Time In	terface Parameters				
Name		IP Address			
Netmask		Broadcast			
MTU		Activate at boot?	💿 Yes 🔿 No		
Create					

Figure 5 - 11 The Create Bootup Interface screen



Caution: If the IP Address for the eth0 NIC is changed, you may lose connection to your RiskFilter Appliance.

Routing and Gateways

You can set the interface and Gateway that you want to act as your default within the Routing and Gateways screen:

Routing and Gateways					
Routing configu	rration acti	vated at <i>boot time</i>			
Default routes	Interface	Gateway			
	eth0 💌	192.168.86.220			
	~		-		
Act as router?	🔿 Yes 📀	No	-		
Static routes	Interface	Network	Netmask	Gateway	
Local routes	Interface	Network	Netmask		
Save				d	

Figure 5 - 12 The Routing and Gateways screen



To configure routing and gateways:

- 1 Select Routing and Gateways from the Network Configuration tab.
- 2 For each route, choose the interface from the drop-down list box and enter the corresponding gateway's IP address into the Gateway field. You can enter up to two default routes.

Default routes	Interface	Gateway
	eth0 💌	192.168.86.220
	~	

- 3 Specify whether you want the RiskFilter System Management Console server to act as a router. You can also specify static and local routes if necessary.
- 4 Click **Save** once you have entered your settings.

DNS Client

This module enables you to configure your system's resolver settings:

DNS Client Option	LS				
Hostname	lasa	Resolution order	Hosts 💙 DNS 👻	~	× ×
DNS servers	198.41.0.4 192.228.79.201 192.33.4.12 128.8.10.90 192.203.230.10 V	Search domains	○ None ⊙ Listed surfcontrol.com	<	

Figure 5 - 13 The DNS Client screen

To configure the DNS Client:

- 1 Select DNS Client from the Network Configuration tab.
- 2 Enter the hostname of your DNS server in the Hostname field.
- 3 Enter the IP addresses of your DNS servers into DNS servers fields.
- 4 Set the Resolution order using the drop-down list boxes then choose from the None or Listed options. If you choose Listed you must enter the domains that you want the server to search in the pane beneath.

DNS Client					
DNS Client Opt	ions				
Hostname	lasa	Resolution order	Hosts 🔽 DNS 👻 🔍	Y Y	~
DNS servers	198.41.0.4 • 192.228.79.201 • 192.33.4.12 • 128.8.10.90 • 192.203.230.10 •	Search domains	○ None ⊙ Listed surfcontrol.com	× ×	
Save					

Figure 5 - 14 The DNS Client screen

5 Click Save.



Host Addresses

You can add new RiskFilter System Management Console hosts to the Host Addresses screen.

To add hosts:

- 1 Select Host Addresses in the Network Configuration tab.
- 2 In the Host Addresses screen, select Add a new host address.

dd a new host address			
IP Address	Hostnames		
127.0.0.1	lasa.surfcontrol.com lasa localhost.localdomain localhost		
192.168.86.198	register.surfcontrol.com surflicense.surfcontrol.com		
92.168.111.48	listsry.surfcontrol.com		

Figure 5 - 15 Host Addresses

3 In the page that follows enter the IP address and name of your new RiskFilter System Management Console host.

reate Host Addre	SS	
Host and Addresses		
IP Address Hostnames	A	
	Y	
	Create	

Figure 5 - 16 Create a Host Address

- 4 Click Create.
- 5 If you want to edit an existing Host Address, click the IP address and edit the details in the screen that follows:

Edit Host /	Address	
Host and Ad	dresses	
IP Address	127.0.0.1	
Hostnames	lasa.surfcontrol.com	
	Save Delete	

Figure 5 - 17 Editing a Host Address

6 Click Save.

RUNNING PROCESSES

This screen tells you which processes are currently running, as well as when it first started up and the command used to run it:

Running Processes						
Display: PID User Memory CPU Search						
Process ID	Owner	Started	Command			
1	root	Aug08	init [3]			
4	root	Aug08	[keventd]			
5	root	Aug08	[ksoftirqd/0]			
6	root	Aug08	[ksoftirqd/1]			
7	root	Aug08	[kswapd]			

Figure 5 - 18 The Running Processes screen

SYSTEM TIME

The system time must be correct in order for licensing and updating to be trouble-free. To do this, the server must use the Time Protocol. Information about this protocol can be seen at:

http://www.tf.nist.gov/service/its.htm

RiskFilter does not support the use of NTP servers. You can reset the system time and timezone in the System Time screen:

System Time					
System Time					
Day	Date	Month	Year	Hour	
Friday	9 🔽	September 🖌	2005 🛩	22 💙 : 06 💙 : 35 💙	
Apply					
Time Serve	er				
Host/Addre	ss s2k.time.edu.cn		、 、		
Sync system time					
Timezone					
Current loca	ation Australia 🔽	Adelaide 🔽			
Change 1	timezone				

Figure 5 - 19 The System Time screen

To reset the system time:

- 1 Select **System Time** in the **System** tab.
- 2 Choose the date, month, year and hour from the drop-down list boxes in the System Time section.
- 3 Click Apply.
- 4 Enter the host name or IP address of the machine that you will use as your time server into the Time Server secton.



- 5 Click **Sync system time**.
- 6 Specify where the RiskFilter System Management Console server is located by choosing from the Current location list boxes in the Timezone section.
- 7 Click **Change timezone** to make the changes. Restart the RiskFilter appliance.

SYSTEM AND SERVER STATUS

Enables you to add monitoring of different types by enabling you to:

- Set up watchdog scripts These can monitor the system and notify the administrator of problems such as low disk space, low memory and dead processes.
- Set up monitoring to run at certain times automatically This can be useful to restart any dead processes or remove unnecessary files, to clean up disks.



THE RISKFILTER TAB

This chapter explains how to use the RiskFilter tab to manage the configuration of services as well as backing up and updating of the software.

WHAT CAN BE CONFIGURED IN THE RISKFILTER TAB?

The RiskFilter tab enables you to:

- Start, stop and restart RiskFilter. You can also see the status of the services.
- Make copies of your RiskFilter configuration. Back up files on a real-time basis, or set a schedule so
 these files are backed up automatically at pre-set times.
- Set up the RiskFilter appliance as a node in a cluster.
- Manage access to the two HTTP servers: Webmin, Administrator Console and Personal E-mail Console. Access can be set to be by HTTP and HTTPS.
- Download the latest version of the RiskFilter software as you did when you first set up RiskFilter.



Figure 5 - 20 The RiskFilter tab

In this tab you have access to the following modules:

- RiskFilter Services Manager
- RiskFilter Backup Manager
- RiskFilter Cluster Wizard
- RiskFilter Web Access Manager
- Update RiskFilter E-mail

See the following sections for detailed information on what can be configured with these modules.



RISKFILTER SERVICES MANAGER

Enables you to start, stop and restart RiskFilter. This screen also gives you the status of the following services:

- Msoftsmg The mail processor and SMTP server
- Msoftadmin The user interface
- Msoftnp.dc The document convertor (extracts text from .docs/.pdfs/.exl files)
- Avagent.mcafee The McAfee Anti-Virus engine

RISKFILTER BACKUP MANAGER

The Backup Manager enables you make a copies of your RiskFilter configuration. You can back up files on a real-time basis or set a schedule whereby these files are backed up automatically at pre-set times:

chedule Backups on Appl	iance		
cneduing backups will allow you to keep y	our Ruskruter - E-mail configuration stored for sale keeping. Later you can download backups to a sa	e location of rest	ore your backups.
Configure Scheduled Backups			
inable Scheduled Backups?	Yes ○ No		
ackup Schedule	Every Month V		
Apply Schedule			
Backup Now			
Pastup Files on Appliana			
аскир г нез он аррнансе			
he following lists the files that are currently :	tored on your appliance. You can use this menu to clean these files out, download them to your local r	nachine or use the	em to restore your syste
he following lists the files that are currently : efore you restore be sure that the RiskFilter	tored on your appliance. You can use this menu to clean these files out, download them to your local 1 - E-mail filtering software is shut down.	nachine or use the	em to restore your syste
he following lists the files that are currently s efore you restore be sure that the RiskFilter file Name(s)	tored on your appliance. You can use this menu to clean these files out, download them to your local r - E-mail filtering software is shut down. Correnan	nachine or use the	em to restore your syste
he following lists the files that are currently s efore you restore be sure that the RiskFilter file Name(s) Boackuo-2005-8-19-13-38-57.mo	tored on your applance. You can use this menu to clean these files out, download them to your local at - E-mail filtering roftware is shut down. Commany. Restore	nachine or use the Is Delete	em to restore your syste
he following lists the files that are currently s effore you restore be sure that the RiskFilter He Name(s) Bbackup-2005-8-19-13-38-57.zip Backup-2005-8-19-15-37-20.zip	tored on your applance. You can use this menu to clean these files out, download them to your local i - E-mail filtering software is shut down. Comman Restore Restore	nachine or use the Is Delete Delete	m to restore your system Download Download
he following lists the files that are currently effore you restore be sure that the RiskFilter the Name(s) Bbackup-2005-8-19-13-38-57.zip Bbackup-2005-8-19-15-37-20.zip Bbackup-2005-8-20-1-59-1.zip	tored on your appliance. You can use this menu to clean these files out, download them to your local E. F. mail filtering software is shut down.	is Delete Delete	m to restore your syste Download Download Download
he following hits the files that are currently s effore you restore have that the Ruk/Eller file Name(s) fbackup-2005-8-19-13-38-57 mp fbackup-2005-8-201-59-1 mp fbackup-2005-8-20-1-59-1 mp fbackup-2005-8-21-159-0 mp	tored on your appliance. You can use this menu to clean these files out, download them to your local at - E-mail filtering software is shut down. Command Restore Restore Restore Restore Restore Restore	is Delete Delete Delete Delete Delete	m to restore your system of the second system of th
he following lists the files that are currently effore you restore be sure that the Euk/Filtes file Name(s) mackup-2005-8-19-13-38-57 mp mackup-2005-8-19-15-37-20 mp mackup-2005-8-20-1-59-1 mp mackup-2005-8-20-1-59-0 mp mackup-2005-8-22-1-59-0 mp	oord on your applance. You can use this menu to clean these files out, download them to your local at - E-mail filtering software is shut down. Comman Restore Restore Restore Restore Restore Restore Restore	is Delete Delete Delete Delete Delete	m to restore your syste Download Download Download Download Download
the following lists the files that are currently effore you restore be sure that the KutkFilter file Nance(). Backupp-2005-8-19-13-38-57.mp Backupp-2005-8-20-1-59-1.mp Backupp-2005-8-20-1-59-1.mp Backupp-2005-8-22-1-59-0.mp Backupp-2005-8-22-1-59-0.mp Backupp-2005-8-22-1-59-0.mp	ored on your applance. You can use this means to clean these files out, download them to your local - E-mail filtering roftware is shut down. Comman: Restore Restor	is Delete Delete Delete Delete Delete Delete	m to restore your syste Download Download Download Download Download Download
he following lists the fleet that are currently effore you restore be nure that the RudeFilter Backup-2005-8-19-13-38-57 aip Backup-2005-8-20-1-59-1 ap Backup-2005-8-20-1-59-1 ap Backup-2005-8-22-1-59-0 ap Backup-2005-8-22-1-59-0 ap Backup-2005-8-21-59-0 ap	ored on your appliance. You can use this mean to clean these files out, download them to your local b - E-mail filtering roftware is shut down. Command Restore Rest	Is Delete Delete Delete Delete Delete Delete Delete Delete Delete	m to restore your syste Download Download Download Download Download Download Download
he following lasts the flar that are currently effore you restore be sure that the Ruk/Filter Hackup-2005-8-19-13-38-57 ap thackup-2005-8-20-1-59-1 zip thackup-2005-8-20-1-59-1 zip thackup-2005-8-21-59-0 zip thackup-2005-8-21-59-0 zip thackup-2005-8-23-1-59-0 zip thackup-2005-8-23-1-59-0 zip	ored on syour appliance. You can use this mean to clean these files out, download them to your local at - E-mail filtering software is shut down. Comman Restore Restore Restore Restore Restore Restore Restore Restore Restore Restore Restore Restore Restore Restore Restore Restore	s Delete Delete Delete Delete Delete Delete Delete Delete	m to restore your syste Download Download Download Download Download Download Download Download
he following lists the files that are currently effore you rentore be sure that the EucliPite file Name() thatcharp-2005-8-19-13-38-57 ap thatcharp-2005-8-20-1-59-1 ap thatcharp-2005-8-21-59-0 ap thatcharp-2005-8-21-59-0 ap thatcharp-2005-8-21-59-0 ap thatcharp-2005-8-21-59-0 ap thatcharp-2005-8-25-159-0 ap thatcharp-2005-8-25-159-0 ap	ord on your appliance. You can use this mean to clean these files out, download them to your local - E-mail filtring software is shut down. Command Restore	is Delete Delete Delete Delete Delete Delete Delete Delete Delete	m to restore your syste Download Download Download Download Download Download Download Download Download
he following lasts the file is that are currently effore you restore be sure that the RuskFilter Handrap-2005-8-19-13-38-57 sip thackap-2005-8-21-15-97-20 ap thackap-2005-8-21-15-90-ap thackap-2005-8-22-1-590-ap thackap-2005-8-22-1-590-ap thackap-2005-8-22-1-590-ap thackap-2005-8-21-1590-ap thackap-2005-8-25-1-590-ap thackap-2005-9-1-1-590-ap thackap-2005-9-1-1-590-ap	ored on your appliance. You can use this mean to clean these files out, download them to your local at - E-mail filtering roftware is shut down. Comman Restore Restore Restore Restore Restore Restore Restore Restore Restore Restore	source of use the second secon	m to restore your syste Download Download Download Download Download Download Download Download Download
The following later the files that are currently lefore you restore be sure that the RukFilter File Narce() thackup-2005-8-19-13-38-57.20 ap thackup-2005-8-21-13-20 ap thackup-2005-8-21-13-90.20 p thackup-2005-8-221-13-90.20 p thackup-2005-8-221-13-90.20 p thackup-2005-8-221-13-90.20 p thackup-2005-8-231-13-90.20 p thackup-2005-9-11-13-0.20 p thackup-2005-9-11-13-0.20 p Cestore from Local File Is this dualog to restore from a backup file	ord on your appliance. You can use this mean to clean these files out, download them to your local - E-mail filtering software is shut down. Command Restore Restore Restore Restore Restore Restore Restore Restore Restore Restore Restore Restore	is Delete Delete Delete Delete Delete Delete Delete Delete Delete Delete	m to restore your syste Dewnload Download Download Download Download Download Download Download

Figure 5 - 21 The RiskFilter Backup Manager screen

To schedule a backup:

- 1 Select RiskFilter Backup Manager in the RiskFilter tab.
- 2 Select Yes in the Enable Scheduled Backups? section.

Configure Scheduled Backups				
L	Enable Scheduled Backups?	Yes ○ No		

Figure 5 - 22 Enabling a backup on the Appliance

3 Select when you want the backup to be performed from the Backup Schedule list box

Backup Schedule	Every Month 🛩
Apply Schedule	Every Day Every Week
Backup Now	Every Month



4 Click **Apply Schedule**. If you want to perform an immediate backup of your files, click **Backup Now**. View these files in the Backup Files on Appliance section:

Backup Files on Appliance				
The following lists the files that are currently stored on your appliance. You can use this menu to clean these files out, download them to your local machine or use them to restore your system. Before you restore be sure that the RiskFilter - E-mail filtering software is shut down.				
File Name(s) Commands				
rfbackup-2005-8-19-13-38-57.zip Restore Delete Download				
rfbackup-2005-8-19-15-37-20.zip Delete Download			Download	
rfbackup-2005-8-20-1-59-1.zip	Restore	Delete	Download	

Figure 5 - 24 The Backup Files on Appliance section

- 5 Enter the path to the backup file into the field or click **Browse** to navigate to it. You can use this to restore your settings to the RiskFilter System Management Console server.
- 6 Click Restore.

RISKFILTER CLUSTER WIZARD

The RiskFilter Cluster Wizard provides a way to synchronize several RiskFilter appliances with a single policy. It also allows for a single administration interface and logging storage center. Once a RiskFilter cluster is configured, you will need to set up load balancing for the mail processing nodes in the cluster. The appliance can be configured into three modes:

- Master A server that gathers all logging information, the master may or may not process spam.
- Slave A server that processes e-mail and reports everything to a master server.
- Original configuration The configuration that is in place before you make any changes to RiskFilter.

To use the Cluster wizard:

- 1 Click the RiskFilter Cluster Wizard module in the RiskFilter tab.
- 2 Choose a running mode from the list box then click **Start**.
- 3 The wizard will ask you for specific information, depending on what type of mode you have asked for:
 - Configure Slave You will be asked to specify:
 - Slave IP the IP address of the slave. This machine must bind to an interface on this RiskFilter appliance.
 - Master IP the IP address of the master server to report to.
 - Configure Master You will be asked to specify:
 - Master IP the IP address of the master server. This machine must bind to an interface on this RiskFilter appliance.
 - Slave IPs the list of slave IPs that will be reporting to this master.
 - Master processes E-mail select this if you want the master to process e-mail. This will
 increase the master load substantially.
 - **Restore Original Configuration** restores the configuration that was in existence before you configured this machine to be a Master or Slave.
- 4 Click Complete.



Load balancing with RiskFilter

Once you have configured your RiskFilter cluster, you can set up load balancing using MX records:

- 1 On the DNS server hosting your domain, create an MX record for each primary RiskFilter server using the same MX preference.
- 2 Give the failover server a higher number. This will give it a lower preference.

Table 5-1 shows an example of MX preference assignments for load-balancing and failover using MX records.

Table 5-1	Using MX	Records for	Load-Balancing
-----------	----------	-------------	----------------

Mail Exchanger	IP Address	MX Preference		
Site A				
mx1.siteA.com	208.126.216.20	5		
mx2.siteA.com	208.126.216.21	5		
mx3.siteA.com	208.126.216.22	5		
mx4.siteA.com	197.201.56.201	10		
Site B				
mx1.siteB.com	197.201.56.201	5		
mx2.siteB.com	197.201.56.202	5		
mx3.siteB.com	197.201.56.203	5		
mx4.siteB.com	208.126.216.20	10		



Figure 5-25 Load balancing

A lower MX preference number gives higher priority than a lower one. In Figure 5-25, e-mail is sent in the following way:

- E-mail sent to site A.com round-robins between mail exchangers 1, 2, and 3, because each RiskFilter appliance has the same MX preference of 5.
- The same thing happens for e-mail sent to site B.com. If site A is down (e.g., with a network failure), the sending mail server will route e-mail to the fourth (failover) MX record, which is the address of a server in a different physical location.

For the described failover to work properly, RiskFilter appliances at site A are configured to accept messages for site B, and RiskFilter appliances at site B are configured to accept messages for site A.

The failover servers have static routes configured so that RiskFilter knows where to route the e-mail. There are also advanced load-balancing switches that can be used for these purposes. These switches offer a variety of load-balancing algorithms, in addition to round-robin delivery, which provide efficient load distribution and timely failover. Using load-balancing switches may improve the overall efficiency of your SMTP infrastructure.

RiskFilter in a cluster set up. You can set up RiskFilter in a cluster and use the wizard to set the IPs of the master and slave/s:



Figure 5 - 26 RiskFilter in a cluster set up

- Internet E-mails coming into slave. Slaves can only be accessed via port 25 from the internet.
- Network 1 Used for communication between master and slave.
- **Network 2** The network where the internal servers lie. This network holds mail servers and the RiskFilter administration clients.

To configure multiple NICs, see Multi-NIC configuration in RiskFilter on page 142.



RISKFILTER WEB ACCESS MANAGER

The Web Access Manager manages two HTTP servers: Webmin and the Administrator Console. Access can be set to be by HTTP and HTTPS.

To set up the access:

- 1 Select Web Access Manager in the RiskFilter tab.
- 2 Select **Require HTTPS Access** or **Require HTTP Access** in the Webmin HTTP Configuration section.
- 3 Click Apply.

RiskFilter Web Access Manager					
This module allows you to configure the Webmin and RiskFilter - E-mail Admin Console HTTP servers' SSL preferences.					
Webmin HTTP Configuration					
Select Access Type 💿 Require HTTPS Access 🔿 Require HTTP Access					
Apply					
RiskFilter - E-mail Admin Console HTTP Configuration					
Select Access Type 📀 Require HTTPS Access 📀 Require HTTP Access					
Apply					

Figure 5 - 27 The RiskFilter Web Access Manager



Note: Clicking Apply saves changes to the configuration files and the appropriate services is restarted. Any connections made during this time will be lost.

- 4 Select Require HTTPS Access or Require HTTP Access in the RiskFilter Console HTTP Configuration section.
- 5 Click **Apply**.



UPDATE RISKFILTER - E-MAIL

This screen is where you can download the latest version of the RiskFilter software as you did when you first set up RiskFilter. There is more information about this facility in the Starter Guide.

Jpdate Now		
lse this menu to download the latest sys	tem updates from a SurfControl plc server.	
Jpdate Items		
RiskFilter - E-mail		
Current Version	Last Update Time	Last Update Status
5.2	08/04/2006 18:42:53	Up to date
SurfControl OS		
Current Version	Last Update Time	Last Update Status
	08/04/2006 00:39:49	Up to date

Figure 5 - 28 The Update RiskFilter-E-mail screen



KEY POINTS

The following list is a summary of the main points covered in Chapter 5. Use this list as a quick reminder of what you can do within the RiskFilter System Management Console:

- To open the RiskFilter System Management Console: Open a web browser and enter: https://<hostname_or_ipaddress>:10000/
- Use the Webmin Actions Log to generate reports on actions carried out by users within any of the modules such as changing passwords, booting up and shutting down the computer and configuration issues.
- Use IP Access Control to only allow access to the appliance from IP addresses that you trust.
- You can change the language of titles, prompts etc that will be displayed in within the RiskFilter appliance interfaces.
- You can specify which IP addresses and port the RiskFilter System Management Console will bind to.
- Webmin can keep records of changes made within the RiskFilter System Management Console.
- The RiskFilter System Management Console needs to connect to the Internet to operate correctly. If you use a proxy server to access Web and FTP sites on the Internet you need to tell Webmin about these machines.
- The Webmin Servers Index enables you to monitor multiple RiskFilter appliances wthout you having to remember the password for each appliance. This feature is only relevent if you have several RiskFilter appliances.
- You can add servers to the Webmin Servers Index using the Webmin Servers Index module.
- Use the Bootup and Shutdown screen to immediately reboot or shut down the system by clicking the relevant button.
- You can use the Change Password screen to change the password of the rfmngr account.
- Historic System Statistics enable you to view real time and historic monitors of system usage.
- Multi Gateway Policy Routng enables you to override the default gateway setting in your routing table. Connections forwarded to RiskFilter will have their packets routed back through the source's configured gateway.
- You can specify what network interfaces are activated at Boot Time.
- You can set the interface and Gateway that you want to act as your default.DNS enables you to configure your system's resolver settings.
- You can add new RiskFilter System Management Console hosts.
- Running Processes tells you which processes are currently running, as well as when it first started up and the command used to run it.
- The system time must be correct in order for licensing and updating to be trouble-free.

- System and Server Status enables you to add monitoring of different types by enabling you to:
 - Set up watchdog scripts These can monitor the system and notify the administrator of problems such as low disk space, low memory and dead processes.
 - Set up monitoring to run at certain times automatically This can be useful to restart any dead processes or remove unnecessary files, to clean up disks.
- RiskFilter Services Manager enables you to start, stop and restart RiskFilter.
- The Backup Manager enables you make a copies of your RiskFilter configuration.
- The RiskFilter Cluster Wizard enables you to set up the RiskFilter appliance as a node in a cluster.
- The Web Access Manager manages two HTTP servers: Webmin and the Administrator Console. Access can be set to be by HTTP and HTTPS.



Appendix

Using the Command Line Interface	. page	158
Internet Threat Database Categories	. page	165



USING THE COMMAND LINE INTERFACE

'rfmngr' is a non-root Linux user on the RiskFilter appliance. It is created in all out-of-the-box RiskFilter appliances and has the default password "\$rfmngr\$". For security reasons this password must be changed as soon as possible. To access the command line interface in order to use the utilities that it offers you need to log in as 'rfmngr'. The utilities available within this interface are all stored in:

/opt/riskfilter/smg/bin

Command: # ssh rfmngr@<RiskFilter-appliance-IP-or-host>

Use 'sudo' to execute any of the commands.

- qtool.sh command line management for the RiskFilter receive queue
 # sudo /opt/riskfilter/smg/bin/qtool.sh
- smgd reports the status of the RiskFilter application
 # sudo /etc/init.d/smgd status



QTOOL.SH

qtool.sh is the Receive Queue Management Utility and provides the command line management for the RiskFilter receive queue.

Command: /opt/riskfilter/smg/bin/qtool.sh -h -l -d -e -i -c

-h - launch help

-1 [filter clause] - list messages in receiving queue

-d - delete messages

-e [export path] - export messages

-i - import messages to queue

-c - clean queues

Example 1 - cleaning queues

```
Command:./qtool.sh -c
# ssh rfmngr@riskfiter-appliance
# sudo /opt/riskfilter/smg/bin/qtool.sh -c
All data inside queue will be cleaned!
Do you want to clean the Queue? (y/n):
y
format queue finished
```

Example 2 - exporting the mails of RQ into a predefined directory

```
Command: ./qtool.sh [export path]
# ssh rfmngr@riskfiter-appliance
# sudo /opt/riskfilter/smg/bin/qtool.sh -e /var/log
Usage: ./qtool.sh [export path]
Do you want to export? (y/n):
y
log priority = com.messagingsoft.storm.util.logger.Priority@56a499
log path = log
log entries = 1048576
Use checkPoint to seek 205282750
Message Position:
```



Queue Id = 4 SegmentOffset = 184259131 SegmentDataOffset = 184259155 Message Id = 3944800 Message Position:

Queue Id = 4 SegmentOffset = 189968858 SegmentDataOffset = 189968882 Message Id = 3945000 Message Position:

```
Queue Id = 4
SegmentOffset = 190975798
SegmentDataOffset = 190975822
Message Id = 3945200
Message Position:
```

Example 3 - importing messages to the receive queue. You must stop the RiskFilter service before the import.

```
Command: ./importmsg.sh [import path]
# ssh rfmngr@riskfiter-appliance
# sudo /etc/init.d/smgd stop
Stopping Msoft admin: [ OK ]
Stopping Msoft npdc: [ OK ]
Stopping Msoft npav: [ OK ]
Stopping Msoft smg: [ OK ]
[root@smg bin]# ./importmsg.sh /tny
Usage: ./importmsg.sh [import path]
Do you want to import? (y/n):
У
now start Q server
log priority = com.messagingsoft.storm.util.logger.Priority@cd2c3c
log path = log
log entries = 1048576
Use checkPoint to seek 776408
total Queue recovery time = 30ms
allocate 3 segment buffers
session timeout = 15 minutes
import message complete
```



```
# sudo /etc/init.d/smgd start
A mysqld process already exists
Starting Msoft smg: [ OK ]
Starting Msoft admin: [ OK ]
```

Example 4 - listing all messages in the receive queue. You can also list messages using a specified filter.

```
Command: /qtool.sh -1
# ssh rfmngr@riskfiter-appliance
# sudo /opt/riskfilter/smg/bin/qtool.sh -1
Do you want to list message? (y/n):
y
message 2073 recieved at 2004/08/16 23:44:53 from ip 218.108.178.118 sender is
love@zj.com deliver to [laixy123@taikang.com] size 1287
message 2074 recieved at 2004/08/16 23:44:53 from ip 218.108.178.118 sender is
love@zj.com deliver to [laixy123@taikang.com] size 1531
```

********** total 2 messages listed *********

Example 5 - Deleting the mails in the receive queue. The RiskFilter service needs be stopped before the deletion



APPENDIX Using the Command Line Interface

sudo /etc/init.d/smgd start
A mysqld process already exists
Starting Msoft smg: [OK]
Starting Msoft admin: [OK]



UNINSTALL.SH

You must run this command under 'root'. This command uninstalls RiskFilter software and is located in / opt/riskfilter/smg/bin. It will remove features installed by InstallAnywhere but will not uninstall files and folders created after the installation.

Example 6 - uninstalling the RiskFilter software

```
[root@smg bin]# ./uninstall.sh
Stopping Msoft admin: [ OK ]
Stopping Msoft npdc: [ OK ]
Stopping Msoft npav: [ OK ]
Stopping Msoft smg: [ OK ]
Preparing CONSOLE Mode Installation...
```

```
______
```

Riskfilter	Secure	Message	Gateway	(created	with	InstallAnywhere	by	Zero	G)

About to uninstall...

PRESS <ENTER> TO CONTINUE:

Uninstalling...



...* * ***** ******* ******* ****** ...* * ***** ****** ******* ******* ...* * ********* ****** ******* ****** Uninstall Complete _____

All items were successfully uninstalled.



INTERNET THREAT DATABASE CATEGORIES

Table 1 shows a summary of the Internet Threat Database Categories:

Table 1 Internet Theat Database Categories

Category	Summary
Core / Liability Categories	 Adult Gambling Illegal Material Offensive
Productivity Categories	 Chain letters Games / interactive Novelty software Computing / Internet Health / medicine Personal / dating Entertainment Phishing / fraud Products / services Finance / home business Humor Special events Other



CORE / LIABILITY CATEGORIES

Table 2 describes the Core/Liability categories. These are the categories that could result in legal or confidentiality issues should a user be accessing them.

Table 2 Core / Liability categories

Category	Media Type	Definition
Adult	 Executable Graphics Movies Sound Text 	 Adult humor, erotic stories, cartoons and animation or erotic chat Adult products including sex toys, CD-ROMs and videos Child Pornography Depictions or images of sexual acts, including sadism, bestiality or any form of fetish Sexually exploitative or sexually violent text or graphics Sexually oriented or erotic full or partial nudity
Gambling	ExecutablesText	 Online gambling or lottery sites that invite the use of real or virtual money Virtual casinos Fantasy sports leagues, sports picks and betting pools Information or advice for placing wagers, participating in lotteries, or gambling, or running numbers
lllegal Material	 Executables Graphics Movies Text 	 Advice on performing illegal acts or obtaining illegal objects Advocating, instructing, or giving advice on performing illegal acts such as phone, service theft, evading law enforcement, lock-picking, fraud, plagiarism/cheating, and burglary techniques Displaying, selling, or detailing the use of guns, weapons, ammunition or poisonous substances Displaying, selling, or detailing use of drug paraphernalia- Hacking
Offensive	 Executables Graphics Movie Sound Text 	 Promoting a political or social agenda that is supremacist in nature and exclusionary of others based on their race, religion, nationality, gender, age, disability, or sexual orientation (e.g. bigotry and racism) Grotesque depictions Offensive jokes and humor
		•



PRODUCTIVITY CATEGORIES

Table 3 describes the Productivity Categories. These are the categories that are not dangerous to company confidentiality or legality, but could result in loss of band-width and productivity should users be accessing them too often.

Table 3 Productivity Categories

Category	Media Type	Description
Chain Letters	ExecutablesText	Mass e-mailed chain letters
Computing/ Internet	 Executables Graphics Movies Sound Text 	 Spy Software Hardware and Software advertisements Web Hosting and Web Design services Questionnaires
Entertainment	 Graphic Text- 	 Entertainment and celebrity news Promotions Horoscopes, Psychic readings and Chinese Astrology Hobbies and recreation
Finance /Home Business	 Executables Graphics Movies Text 	 Get Rich Quick schemes and Multi-Level Marketing Debt consolidations and refinance schemes Mortgage and Loans promotional services Stock quotes, stock tickers, and fund rates Term Life Insurance Work-at-Home Business reports & promotions
Games / Interactive	GraphicsText	 Online games and puzzles Interactive quizzes, movies and programs
Health / Medicine	GraphicsText	 Prescription medicines promotions (e.g. Viagra Ordering) Weight Loss, health supplements Medical product promotions Medical, dental and health Insurance Body modification and sexual enhancements
Phishing / fraud	 Graphics Movies Sound Text 	 Virus hoaxes Phishing scams Deceptive or fraudulent information Urban legends (e.g. 419 scam and International Lottery scam)
Humor	ExecutablesGraphicsMovies	 Jokes and pranks (non-sexually explicit) Humorous and satirical awards Cartoons and humorous pictures
Novelty Software	• Text	 Cursor-changing software Other software and gadgets intended for entertainment value rather than system performance
Personal /Dating	• Text	 Singles listings, matchmaking and dating services Personal chat lines
Products / Services	 Executables Graphics Movies Text 	 General product & service sales and advertisements Promotions and commercials
	•	•



Table 3 Productivity Categories

Category	Media Type	Description
Special Events	 Graphics Movies Sound Text 	 Festive and Seasonal messages, files, promotions Messages pertaining to a current event that may be objectionable based on content, bandwidth, or negative impact on productivity such as a major sports event
Other	• Text	 Items that do not fit into the above categories Job Search E-greeting cards and wishes Questionnaires, polls and surveys Stories, quotes, riddles, quizzes
	•	•

INDEX

A

accept e-mail for relay from the following ips 30 actions if filter triggered 71 add/edit phrase 74 admin console locale 12 admin console session timeou 12 allow access list 28 archive level 25 avagent.mcafee 149

B

bypass rbl checks 28

С

certificate signing request 26 copy to 67 core / liability categories 165, 166 cpu 139 csr 26 custom certificate 26

D

days to keep log files 24 days to keep messages 25 deliver message 68 deliver message 35 delivery log 110 dfp 83, 85 dictionary management 3 directory to store messages 25 distributed processing systems 107 dns client 144 drop connection 29 drop message 68 drop message 35 dynamic white list 39

E

exporting

Black List 38 Certificate Signing Request 26 Certificates 26 dictionary 78 exporting the mails of rq 159

F

fully qualified domain name 145

H

heuristics 83, 85, 86 host addresses 145 http proxy 137

I

import a surfcontrol dictionary pack 76 import a unicode text file 76 import from an ldap server 70 import from file 70 import-export utility 77 importing Address Lists 69 Black List 37 Certificates 26 unicode text file 77 White List 39 interfaces 136 ip access control 135 isolate message 35

K

keep maximum storage size at ... 24, 25

L

language Admin Console Locale 12 dictionary 73 last update attempt 56 last update status 56 latest definitions 56 lexirules 83, 85, 87 license expiry date 56 limit data size per connection 35 load balancing 41 logical operators 94, 94, 94

M

managed modules 47 management console 132 managing messages 46 master 150 master/slave cluster configuration 137 mcafee 83 message log 110 message statistics 106 microsoft active directory 15 modify subject 67 msoftadmin 149 msoftnp.dc 149 msoftsmg 149

N

network interfaces 141 no proxy for 137 notification message 48 notifications 25

0

open message 75 open relay 30 operands 95 original configuration 150

P

patterns 97 pem 48 policy recursion 79 preferred mime charse 12 productivity categories 165, 167

Q

qtool.sh 158 queues 71

R

rbl 28 real-time blacklist 28 recipient e-mail address validation 33 reprocess messages 125 reset counter 116 reverse dns 28 riskfilter system management console 132 routing and gateways 143

S

save to isolate message 68 save to spam message 68 save to virus message 68 security verification 43 send notification 68 sensitivity level 86 slave 150 smgd 158 smtp greeting delay 28 smtp greeting message 12 spf record 30 standard disclaimer 90 support screen 61 system status 106

Т

threshold 73 timeout 23 timezone 147 tls verification 25 today's report 110 total simultaneous connections 23 transport layer security 42

U

undeliverable messages 43 using logical operators 94 using the expression list 93

V

valid domain 33 valid keyword expression examples 95 validation settings 18 view report 110

W

watchdog scripts 147 webmin actions log 135

Х

x header 67

Z

zip log files older than... 24

NOTICES

Updates to the SurfControl documentation and software, as well as Support information are available at www.SurfControl.com/support.

Copyright ©1998-2007 SurfControl plc. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owner. SurfControl is a registered trademark and SurfControl and the SurfControl logo are trademarks of SurfControl plc. All other trademarks are property of their respective owners.

Parts of this program incorporate software with the following licence terms:

OpenSSL

Copyright (c) 1998-2006 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/ or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

SSLeay

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/ or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you

must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OFSUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Sun RPC
 * Sun RPC is a product of Sun Microsystems, Inc. and is provided for * unrestricted use provided that this legend is included on all tape * media and as a part of the software program in whole or part. Users * may copy or modify Sun RPC without charge, but are not authorized * to license or distribute it to anyone else except as part of a product * or program developed by the user.
* SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE * WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR * PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. *
* Sun RPC is provided with no support and without any obligation on the * part of Sun Microsystems, Inc. to assist in its use, correction, * modification or enhancement. *
* SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE * INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC * OR ANY PART THEREOF. *
 * In no event will Sun Microsystems, Inc. be liable for any lost revenue * or profits or other special, indirect and consequential damages, even if * Sun has been advised of the possibility of such damages.
* Sun Microsystems, Inc. * 2550 Garcia Avenue * Mountain View, California 94043 */
* Generic DES driver interface * Keep this file hardware independent * Copyright (c) 1986 The following copyright and usage term text is in the file. #////////////////////////////////////
Copyright (c) 2000-2001 ConnectTel, Inc. All Rights Reserved. # # This file is part of the Abyss library
Redistribution and use in source and binary forms, with or without # modification, are permitted provided that the following conditions
 # are met: # 1. Redistributions of source code must retain the above copyright # notice, this list of conditions and the following disclaimer. # 2. Redistributions in binary form must reproduce the above copyright # notice, this list of conditions and the following disclaimer in the # documentation and/or other materials provided with the distribution. # 3. The name of the author may not be used to endorse or promote products # derived from this software without specific prior written permission.
" # THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS" AND # ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE # IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE # ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE # FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL # DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS # OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) # HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT # LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY # OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF # SUCH DAMAGE. #
######################################
Copyright (c) 1996-2001 - Rosimildo da Silva
Copyright (C) 1998-2003 Daniel Veillard. All Rights Reserved.
in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of

the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial

portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE DANIEL

VEILLARD BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of Daniel Veillard shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

Copyright (c) 1996 - 2007, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

Portions of this Product contains or is derived from:

MD5C.C - RSA Data Security, Inc., MD5 message-digest algorithm

MDDRIVER.C - test driver for MD2, MD4 and MD5

The Apache Software License, Version 1.1

Copyright (c) 2000 The Apache Software Foundation. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/ or other materials provided with the distribution.

3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

"This product includes software developed by the Apache Software Foundation (http://www.apache.org/)."

Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

International Components for Unicode (ICU)

Copyright (c) 1995-2003 International Business Machines Corporation and others

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

Copyright (C) 1999-2005 High Availability Linux Project

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Copyright (C) 2003 Jfree.org

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

Portions of this Product contain or are derived from:

MD5C.C - RSA Data Security, Inc., MD5 message-digest algorithm

MDDRIVER.C - test driver for MD2, MD4 and MD5

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

Expat – XML Parser Toolkit

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

** **

** FILE_NAME

** This file is part of the ABYSS Web server project.

**

** Copyright (C) 2000 by Moez Mahfoudh <mmoez@bigfoot.com>.

** All rights reserved.

**

** Redistribution and use in source and binary forms, with or without

** modification, are permitted provided that the following conditions

** are met:

** 1. Redistributions of source code must retain the above copyright

** notice, this list of conditions and the following disclaimer.

- ** 2. Redistributions in binary form must reproduce the above copyright
- ** notice, this list of conditions and the following disclaimer in the
- ** documentation and/or other materials provided with the distribution.

** 3. The name of the author may not be used to endorse or promote products

** derived from this software without specific prior written permission.

**

- ** THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS" AND
- ** ANY EXPRESS OR IMPLIED WARRANTIES. INCLUDING. BUT NOT LIMITED TO. THE

** IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE

** ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE

** FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL

** DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS

** OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

** HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

** LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY

** OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF

** SUCH DAMAGE.

**

// The copyright notice below refers to the original base 64 code.

// Some modifications are Copyright (C) 1998, 1999 Rik Hemsley rik@kde.org /*

* Original version Copyright 1988 by The Leland Stanford Junior University

* Copyright 1998 by the University of Washington

- *
- * Permission to use, copy, modify, and distribute this software and its
- * documentation for any purpose and without fee is hereby granted,

* provided that the above copyright notices appear in all copies and that

* both the above copyright notices and this permission notice appear in

* supporting documentation, and that the name of the University of

^{*} Washington or The Leland Stanford Junior University not be used in
* advertising or publicity pertaining to distribution of the software

- * without specific, written prior permission. This software is made
- * available "as is", and THE UNIVERSITY OF WASHINGTON AND THE LELAND
- * STANFORD JUNIOR UNIVERSITY DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED,
- * WITH REGARD TO THIS SOFTWARE. INCLUDING WITHOUT LIMITATION ALL IMPLIED
- * WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND
- * IN NO EVENT SHALL THE UNIVERSITY OF WASHINGTON OR THE LELAND STANFORD
- * JUNIOR UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL
- * DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR
- * PROFITS, WHETHER IN AN ACTION OF CONTRACT, TORT (INCLUDING NEGLIGENCE)
- * OR STRICT LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
- * PERFORMANCE OF THIS SOFTWARE.
- */

Note the following block referring to resale of WFC code.

** Author: Samuel R. Blackburn

** Internet: wfc@pobox.com

**

** You can use it any way you like as long as you don't try to sell it. **

- ** Any attempt to sell WFC in source code form must have the permission ** of the original author. You can produce commercial executables with
- ** WFC but you can't sell WFC.

**

** Copyright, 2000, Samuel R. Blackburn

**

** \$Workfile: soap_parameter2.cpp \$

** \$Revision: 1.1 \$

** \$Modtime: 11/09/01 7:45 \$

** \$Reuse Tracing Code: 1 \$

*/

• (C) Copyright Greg Colvin and Beman Dawes 1998, 1999.

· Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Copyright (C) 2003 Jfree.org

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version. This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

SPFJava

Copyright (c) 2004, Mimecast

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Mimecast nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GNU Libidn is an implementation of the Stringprep, Punycode and IDNA specifications defined by the IETF Internationalized Domain Names (IDN) working group, used for internationalized domain names. The Java version is JNet-Tool.jar.

Copyright (C) 2005 Ventruba

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version. This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details. You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

LDAP

The contents of this file are subject to the Mozilla Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtains a copy of the License at http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the license. The Original Code is Idap.jar. The Initial Developer of the Original Code is Netscape Communications Corporation. Portions created by the Initial Developer are Copyright (C) 1998 the Initial Developer. All Rights Reserved.Contributors:Netscape Communications Corporation.